Giving Shape to Ideas

bizhub 36

ユーザーズガイド　セキュリティー機能編



2012. 2
Ver. 1.03

もくじ

1 セキュリティーについて

2 管理者編

3 ユーザー編

4 アプリケーションソフト編

1 セキュリティーについて

1 セキュリティーについて

1.1 はじめに

このたびは弊社製品をお買い上げいただき、ありがとうございます。

このユーザーズガイドには、《bizhub 36》のセキュリティー機能に関する操作方法、使用上のご注意などについて記載しています。本機の性能を十分に発揮させて、効率的にご利用いただくために、ご使用前にこのユーザーズガイドを最後までお読みください。お読みになった後は必ず本機を管理される方が保管しておいてください。万一、ご使用中わからないことや不都合が生じたとき、きっとお役に立ちます。

本ユーザーズガイド（Ver. 1.03）は、bizhub 42/bizhub 36/ineo 42/ineo 36 全体制御ソフトウェア (コントローラーファームウェア：A3EW30G0224、Boot 制御部：A3EW99G0010000) について記載しています。

ISO15408 規格の適合

本機は、セキュリティ強化設定を［する］にすることで、強固なセキュリティー機能が得られます。

本機のセキュリティー機能は、ISO/IEC15408（レベル：EAL3）に適合しています。

操作上のご注意

本機操作中、誤操作および誤入力に対して警告メッセージまたは警告音（ピ音）を発します。（ただし、ユニバーサル設定の音設定にて各設定音を［しない］に設定した場合、「ピ音」等の警告音は発しません。）警告メッセージまたは警告音が発せられた場合、メッセージ等の指示に従い正しい操作および入力を再度行ってください。

本機管理者は、各モードへのアクセス終了後および各モードへのアクセス中、各設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず各モードをログアウトするようにしてください。

本機管理者はユーザーに対し、各モードへのアクセス終了後および各モードへのアクセス中、各モード画面を表示させたままその場を離れる場合、必ず各モードをログアウトするように指示徹底を行ってください。

本機管理者は、設定が重複するおそれがあるため、操作パネルとクライアント PC から同時にログインした状態で本機の設定を変更しないでください。

設置チェックリスト

この設置チェックリストは、本機を設置するサービスエンジニアに対するチェック項目を記載しています。サービスエンジニアは以下のチェックを行い、本機管理者にチェックした項目について説明を行ってください。

サービスエンジニアへのお願い

右側のチェックボックスにチェックを入れ、完了を確認してください。

1.	本機の設置を行う前に、次のことを実施してください。	完了
	本機のセキュリティー機能を強化するかの確認を本機管理者に対して行い、強化したい場合は、以下のチェックを行ってください セキュリティー機能を強化しない場合は、チェックを入れずに完了してください	☐
	本機の設定に関する情報は誰にも漏洩しない、また本機の設置および保守サービスにおいて悪意を持った行為を行わない事を誓います	☐
	本ユーザーズガイド　セキュリティー機能編はセキュリティー対応バージョンであることを確認し、本機管理者に対してセキュリティー対応であることの説明を行い、ユーザーズガイドを提供してください	☐
2.	本機の設置後、サービスマニュアルを参照し、以下の設定を実施してください。	
	CE パスワードの設定を行ってください	☐
	サービスマニュアルにて確認した「コントローラー」および「ブート」のファームウェアバージョンとリビジョンが、ファームウェアバージョン表示画面の値と一致していることを確認してください ファームウェアバージョンおよびリビジョンが一致していない場合、ファームウェアの書き換えが必要であることの説明をし、ファームウェアの書き換えを行ってください	☐
3.	本機の設置後、本ユーザーズガイドを参照し、以下の設定を実施してください。	
	本機管理者によって管理者パスワードの設定が行われたことを確認してください	☐
	本機管理者によってユーザー認証が［デバイス］または［外部サーバー］（Active Directory のみ）に設定されたことを確認してください	☐
	本機管理者によって SSL 通信を行うため、自己証明書の登録が行われていることを確認してください	☐
	本機管理者によってパスワード規約が［する］に設定されたことを確認してください	☐
	本機管理者によりセキュリティ強化設定を［する］に設定してください	☐
	本マニュアルの記載内容についての評価を受けている言語は日本語および英語です 評価対象となった言語のマニュアルの入手方法についての説明を行ってください	☐
	本機セキュリティー機能の設定が完了したことを、本機管理者に対して説明を行ってください	☐

上記チェック完了後、本ページのコピー 1 部をサービス実施店にて保管し、本書を本機管理者にお渡しください。

製品名		会社名	設置先部署名	担当者名
お客様（本機管理者）				
サービス実施店			–	

1.2 セキュリティー機能について

本機は、セキュリティ強化設定を［する］にすることでセキュリティー機能が有効化されます。セキュリティ強化設定の［する］により変更される各セキュリティー機能の設定について詳しくは、2-5 ページをごらんください。

セキュリティ強化設定が［する］に設定された場合、認証機能が強化され管理者設定、ユーザー認証モードおよび機密印刷ファイルへのアクセスに対し、パスワード認証によるアクセス制限を行い、正当な利用者によるアクセスのみを許可します。

パスワードにはパスワード規約の条件を満たしたパスワードのみが設定可能となり、容易に解読可能なパスワードの設定を禁止します。パスワード規約について詳しくは、1-8 ページをごらんください。

認証操作禁止機能によりパスワード認証時、パスワード誤入力の累積回数が 3 回に達した時点で不正アクセスと判断し、以降のパスワード入力操作を禁止します。パスワード入力操作を禁止状態にすることで不正使用や不正なデータの持ち出しを防止し、より安全に本機を使用することを可能にします。ただし本機能は ISO15408 の認証対象にはなっていません。

本機を廃棄またはリース返却する場合、データ消去機能により HDD の全データおよび SSD のデータ領域に上書き消去を行います。また、NVRAM 上に保存されたすべてのパスワードを出荷時設定に戻すためデータの漏洩を防止できます。データ消去機能によりクリアされる項目について詳しくは、1-10 ページをごらんください。

チェック回数クリア条件

認証時における誤入力回数のチェック回数を 0 クリアするには以下の条件があります。

重要
本機の再起動によりチェック回数がクリアされるため、頻繁に電源の ON/OFF を行っているユーザーがいる場合は声をかけるなどの対策を実施してください。

＜管理者設定＞
- 管理者設定の認証に成功した場合
- 本機の再起動を行った場合

＜ユーザー認証＞
- ユーザー認証に成功した場合
- 本機の再起動を行った場合

＜機密印刷＞
- 機密印刷の認証に成功した場合
- 本機の再起動を行った場合

＜ SNMP パスワード（auth-password、priv-password）＞
- SNMP 認証に成功した場合
- 本機の再起動を行った場合

1.3 保護対象となるデータの考え方について

本機におけるセキュリティーの考え方は、「ユーザーの意に反して暴露される可能性のあるデータの保護」です。

本機を利用している間、本機に登録された利用可能な状態にある以下の画像ファイルを保護します。

- 機密印刷により HDD 上に登録される画像ファイル
- HDD 送信により HDD 上に「個人」として登録される画像ファイル
- 認証＆プリントにより HDD 上に登録される画像ファイル

また以下のデータも保護対象資産とします。

- パスワード
  - HDD 上に登録されるユーザーパスワード、機密印刷パスワードおよび NVRAM 上に登録される管理者パスワード、SNMP パスワード
- ユーザー識別情報
  - HDD 上に登録されるユーザー識別情報
- IC カード情報
  - HDD 上に登録されるユーザーの IC カード情報
- 高信頼チャネルの設定データ
  - NVRAM に登録される高信頼チャネルの設定データ
- 外部サーバー識別設定データ
  - HDD に登録される外部サーバー識別の設定データ

本機をリース返却や廃棄するなどにより本機の利用を終えた場合や HDD が盗難にあった場合、HDD、SSD および NVRAM に保存されている以下のデータを保護します。

- 機密印刷により HDD 上に登録される画像ファイル
- HDD 送信により HDD 上に「個人」として登録される画像ファイル
- 認証＆プリントにより HDD 上に登録される画像ファイル
- 待機状態にあるジョブの画像ファイル
- 機密印刷ファイル、HDD 送信により「個人」として登録されるファイル、認証＆プリントファイル以外に HDD データ領域および SSD データ領域に保管される画像ファイル
- 画像ファイルとして利用された、一般的な削除操作だけでは削除されない HDD データ領域および SSD データ領域に残存しているデータファイル
- プリント画像ファイル処理において生成されたテンポラリデータファイル
- 送信宛先データファイル（E-mail アドレス、電話番号）
- NVRAM に保管される管理者パスワード、SNMP パスワード、高信頼チャネルの設定データ、本機の設定データ
- HDD に保管されるユーザー識別情報、ユーザーの IC カード情報、ユーザーパスワード、機密印刷パスワード、外部サーバー識別の設定データ

本機におけるデータ保護方法として、ネットワーク上で送受信する画像（HDD 送信ファイル）の秘匿性を確保するための SSL 機能があります。

オフィス LAN 内の IT 機器間にて秘匿性の高い画像データ（機密印刷ファイル、HDD 送信ファイル、認証＆プリントファイル）を送受信する際に、正しい相手先に対して信頼されるパスを介して通信する、または暗号化しており、セキュリティー対策が要求される組織にも対応したオフィス環境を想定しています。

重要

クライアント PC から本機に送信される機密印刷ファイル、認証＆プリントファイルは暗号化されません。機密印刷ファイル、認証＆プリントファイルを保護するために、暗号通信機器や盗聴検知機器を設置するなど、盗聴防止対策を行ってください。

HDD が盗難にあった場合は、HDD の暗号化機能によりデータは保護されますが、HDD 暗号化機能は保証対象外となります。

1.4 運用管理時のご注意

本機および本機で扱われるデータは、以下の条件が満たされるオフィス環境にて利用されることを想定しています。

管理者の役割および条件

管理者は、本機を管理する上で不当な行為を行わないよう、責任をもって管理を行うこと。

<対策>

- 管理者には、本機を管理する上で不当な行為を行わないよう、責任をもって管理を行える方を 1 人だけ任命してください。
- SMTP サーバー（メールサーバー）または DNS サーバーを利用する場合、各サーバーの管理者により適切に管理され、無断で設定が変更されないよう定期的に確認を行ってください。

パスワードに関する運用条件

管理者パスワード、auth-password、priv-password は、管理者によって漏洩しないよう適切に管理され、容易に推測可能なパスワードを設定しないこと。機密印刷パスワード、ユーザーパスワードはそれぞれのユーザーによって漏洩しないよう適切に管理され、容易に推測可能なパスワードを設定しないこと。

<対策>

- 本機管理者は、管理者パスワード、auth-password、priv-password は管理者以外には絶対に知られないようにしてください。
- 本機管理者は、管理者パスワード、auth-password、priv-password は定期的に変更を行ってください。
- 本機管理者は、管理者パスワード、auth-password、priv-password には誕生日、社員番号等から推測可能な番号を設定しないでください。
- 本機管理者は、ユーザーパスワードの変更を行った場合、速やかに該当するユーザーによってパスワードの変更を行わせてください。
- 本機管理者は、サービスエンジニアによって管理者パスワードが変更された場合、速やかに管理者パスワードの変更を行ってください。
- 本機管理者はユーザーに対して、ユーザー認証、機密印刷に設定されているパスワードは本人以外には知られない運用を実施させてください。
- 本機管理者はユーザーに対して、ユーザー認証に設定されるパスワードは定期的に変更を行わせてください。
- 本機管理者はユーザーに対して、ユーザー認証、機密印刷に設定されているパスワードには誕生日、社員番号等から推測可能な番号を設定させないでください。
- 本機管理者は管理者が交代した場合、速やかに新しい管理者によって管理者パスワードの変更を行わせてください。

本機のネットワーク接続条件

外部ネットワークと接続される場合は、外部ネットワークからの不正な接続を許可しないこと。

<対策>

- 本機が接続されるオフィス内 LAN が外部ネットワークと接続される場合、外部ネットワークから本機へのアクセスを遮断するためにファイアウォール等の機器を設置し、正しく設定を行ってください。
- 本機が接続されるオフィス内 LAN において、無断で他の複写機が接続されることがないよう、常にネットワークの管理を行ってください。

ユーザー情報管理システムの管理条件

本機管理者およびサーバー管理者は、本機および本機が設置されるオフィス内 LAN に接続されるユーザー情報管理システムに対して、パッチの適用やアカウント管理を行い、適切なアクセス制御が実施される運用管理を行うこと。

<対策>

- ユーザー情報管理システムが常に最新の状態となるようパッチを適用してください。
- ユーザーの権限変更に応じて、速やかに該当するアカウント情報を変更してください。
- ユーザーの異動時には、速やかに該当するアカウント情報を削除してください。

セキュリティー機能の動作設定運用条件

管理者は、セキュリティ強化設定が［する］の状態で本機が利用されるよう、運用管理を行うこと。

本機の運用・管理

本機管理者は以下の運用管理を行うこと。

- 本機管理者は、管理者設定での操作終了後、必ず管理者設定をログアウトしてください。また、本機管理者はユーザーに対して、機密印刷ファイルの操作など、ユーザー認証モードでの操作終了後、必ずユーザー認証モードをログアウトする運用を実施させてください。
- 本機管理者は、本機に登録されているデバイス証明書（SSL 証明書）を適切に管理する運用を実施すること。

本機の保守管理

本機管理者は以下の保守管理作業を行うこと。

- サービスエンジニア以外は、本機の物理的な保守管理作業等を行わないよう運用管理を行ってください。
- サービスエンジニアによる物理的な保守管理作業は必ず本機管理者の立会いのもと実施される運用管理を行ってください。
- オプションによっては、セキュリティ強化設定を［しない］にしないと装着できないものがあります。追加オプションを購入時に、セキュリティ強化設定が［する］で運用できるものであるか不明な場合は、サービス実施店にお問い合わせください。

IC カードおよび IC カードリーダーに関する運用条件

本機では以下の IC カードおよび IC カードリーダーをサポートする。

IC カード種類	IC カードリーダー
Type A	AU-201、SCL-010
Felica IDm	AU-201、SCL-010
HID Prox	AU-201H（北米地域のみ）

IC カードリーダーについて、以下の条件で運用を行うこと。

- サービスエンジニアから提供されたものをご使用ください。詳しくはサービス実施店にご連絡ください。
- IC カードリーダーを使用するには、本機にローダブルドライバーをインストールする必要があります。詳しくはサービス実施店にご連絡ください。
- 本機に接続する IC カードリーダーは 1 つです。
- IC カードリーダーが本機の電源投入時に本機に接続されていなかった場合や、電源投入状態で挿き抜しを行った場合の動作保証はいたしません。
- ICカードリーダーが複数種のICカードタイプをサポートしていた場合でも､認証に使用するICカードタイプは 1 種類です。複数種の IC カードタイプを使用した認証の動作保証はいたしません。
- 複数枚の IC カードを同時に IC カードリーダーに読み込ませた認証の動作保証はいたしません。

IC カードの所有条件

本機管理者は組織内に以下の運用を行うことを規定した運用規定が存在し、規定に従った運用が行なわれていることを確認する。

- 本機を利用する組織の責任者は、組織で利用するために発行した IC カードを、その IC カードの所有が許可される正しい利用者へ配布してください。
- 本機を利用する組織の責任者は、利用者に対して IC カードの他人への譲渡、貸与を禁止し、紛失時の届出を徹底させてください。

1.5　その他

パスワード規約について

パスワード規約により、管理者パスワード、ユーザーパスワード、機密印刷パスワード、SNMP パスワードは、同一キャラクタのみのパスワードの登録や変更を受け付けません。また、管理者パスワード、ユーザーパスワード、SNMP パスワードは、現在設定されているパスワードと同一パスワードへの変更を受け付けません。

各パスワードに使用できる桁数およびキャラクタについて詳しくは、下表をごらんください。

重要
セキュリティ強化設定を行う前に、必ずパスワード規約を有効に設定してください。パスワード規約の設定方法は、操作パネルより、[設定メニュー / カウンター] ▸▸ [管理者設定] ▸▸ [↓] ▸▸ [セキュリティ設定] ▸▸ [セキュリティ詳細] で [パスワード規約] を [する] に設定します。

<table>
<tr><th>対象パスワード</th><th>桁数</th><th>キャラクタ</th></tr>
<tr><td>ユーザーパスワード</td><td>8 桁以上</td><td>・ 数字：0 ～ 9
・ 英字：大文字、小文字
・ 記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~、+
合計 93 文字が選択可能</td></tr>
<tr><td>管理者パスワード</td><td>8 桁</td><td>・ 数字：0 ～ 9
・ 英字：大文字、小文字
・ 記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~、+、SPACE
合計 94 文字が選択可能</td></tr>
<tr><td>機密印刷パスワード</td><td>8 桁</td><td>・ 数字：0 ～ 9
・ 英字：大文字、小文字
・ 記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~、SPACE
合計 93 文字が選択可能</td></tr>
<tr><td>SNMP パスワード
・ auth-password
・ priv-password</td><td>8 桁以上</td><td>・ 数字：0 ～ 9
・ 英字：大文字、小文字
・ 記号：!、$、%、&、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、]、^、_、`、{、|、}、~、+
合計 90 文字が選択可能</td></tr>
</table>

各種アプリケーション使用時の注意

各種アプリケーションを使用する場合は、以下の条件を守ってご使用ください。

- PageScope Web Connection をはじめ各種アプリケーションを使用する場合、入力されたパスワードは各アプリケーションのパスワード管理機能により、ご使用の PC に記憶されます。パスワードを記憶させたくない方は、各アプリケーションのパスワード管理機能を無効にしてご使用ください。
  また、PageScope Web Connection をはじめ各種アプリケーションを使用する場合、入力されたパスワードが「*」または「●」として表示される Web ブラウザや各種アプリケーションをご使用ください。入力されたパスワードがそのまま画面に表示される機能があっても使用しないでください。
- PageScope Web Connection をはじめ各種アプリケーションを使用する場合、Web ブラウザではキャッシュを保存しない設定にしてください。
- クライアント PC 側で Internet Explorer などの Web ブラウザをご使用の場合で、SSL 設定を利用する場合は「SSL v2」ではなく、「SSL v3」もしくは「TLS v1」をご使用ください。
- セキュリティ強化設定が [する] に設定されている場合、PageScope Direct Print は使用できません。
- 本ユーザーズガイドに記載されていないオプションのアプリケーションについては、ISO15408 の認証の対象にはなっておりません。

通信の暗号化について

暗号鍵生成においてサポートしている鍵交換方式および通信の暗号化方式のアルゴリズムは以下の通りです。

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

重要

暗号鍵生成時にアルゴリズムを選択することはできません。また SSL 設定はアプリケーション、ブラウザにより自動的に SSLv3 が選択されますので、手動で SSLv2 に設定を変更しないようにしてください。保護対象となるデータの改ざん、漏えいのリスクが高まります。

本機管理者は、SSL 設定が SSLv2 の状態で SSL 暗号化通信が行われることがないよう運用管理を行ってください。

MD5 により電子署名された SSL 証明書は使用しないでください。保護対象となるデータの改ざん、漏えいのリスクが高まります。

適切な強度で SSL 暗号通信を行うには下記ブラウザをご使用ください。下記ブラウザを使用することにより、送受信される画像データの機密性を確保した SSL 暗号通信を実現することができます。

Windows XP, Server 2003, Vista, 7, Server 2008, Server 2008 R2

- Microsoft 「Internet Explorer 6」以降推奨
- Mozilla Firefox 3.6 以降推奨

Macintosh MacOS X

- Mozilla Firefox 3.6 以降推奨

Linux

- Mozilla Firefox 3.6 以降推奨

IPP 印刷について

IPP（Internet Printing Protocol）とは TCP/IP プロトコルの HTTP（HyperText Transfer Protocol）を利用し、機密印刷や HDD に保存されている画像データをインターネット経由で印刷できる機能です。また IPPS（IPP over SSL/TLS）とは、SSL による暗号化通信を行う IPP です。

＜プリンタードライバーのインストール＞

IPP 印刷を行う場合はプリンタードライバーをインストールする必要があります。「プリンタの追加ウィザード」より、「インターネット上または自宅 / 会社のネットワーク上のプリンタに接続する」を選択して「URL」フィールドに、以下の形式で、本機の URL を入力します。設定が完了したプリンタは通常のローカルプリンタと同様に使用することができます。

http:// ＜本機の IP アドレス＞ /ipp
例：本機の IP アドレスが 192.168.1.20 の場合
http://192.168.1.20/ipp

IPPS 印刷に設定するときは
https:// ＜本機の IP アドレス＞ /ipp を入力してください。

＜ Windows Vista/7/Server 2008/Server 2008 R2 での証明書の登録のしかた＞

Windows Vista/7/Server 2008/Server 2008 R2 では、セキュリティー機能が強化されているため、SSL 証明書が証明機関により発行されたものでない場合は証明書のエラーが表示されます。その場合には Windows Vista/7/Server 2008/Server 2008 R2 でコンピューターアカウント用の信頼された発行元の証明書として本機の証明書を登録しておく必要があります。

まず事前に DNS サーバーに本機のホスト名および IP アドレスを登録します。次に PageScope Web Connection における［TCP/IP 設定］で DNS サーバーに登録した DNS ホスト名、DNS デフォルトドメイン名を設定します。

またインポートする証明書は PageScope Web Connection で SSL 暗号通信のための証明書を登録し、公開鍵を含む証明書としてあらかじめエクスポートしておく必要があります。

1 「このサイトの閲覧を続行する」より PageScope Web Connection 画面を表示させます。

2 ［証明書のエラー］をクリックして証明書を表示させ、［証明書のインストール］をクリックして証明書のインストールを行います。

3 物理ストアを表示させて、あらかじめエクスポートしておいた証明書を「信頼されたルート証明機関」内の「ローカルコンピュータ」に配置して、証明書をインポートします。

< Windows Vista/7/Server 2008/Server 2008 R2 での IPPS 印刷設定>

プリンタの追加設定より「https://［ホスト名］.［ドメイン名］/ipp」を入力します。

［ホスト名］と［ドメイン名］は、DNS サーバーに設定した名称を指定してください。

データ消去機能によりクリアされる項目

データ消去機能によりクリアされる項目については以下の通りです。

クリアされる項目	クリア内容	クリア方法
セキュリティ強化設定	セキュリティ強化設定が［しない］に設定される。	全領域上書き削除 SSD 低レベルフォーマット 全設定初期化
ユーザー登録データ	ユーザーに関する登録情報がすべて削除される。	全領域上書き削除
機密印刷パスワード / ファイル	機密印刷に関する登録情報および保存ファイルはすべて削除される。	全領域上書き削除
HDD 送信ファイル	HDD 送信により「個人」として登録されるファイルはすべて削除される。	全領域上書き削除
認証 & プリントファイル	認証 & プリントファイルはすべて削除される。	全領域上書き削除
画像ファイル	・ 機密印刷ファイル、HDD 送信により「個人」として登録されるファイル、認証 & プリントファイル以外に保管される画像ファイル。 ・ 待機状態にあるジョブの画像ファイル。 ・ 画像ファイルとして利用された、一般的な削除操作だけでは削除されない残存データファイル。 ・ プリント画像ファイル処理において生成されたテンポラリデータファイル。	全領域上書き削除 SSD 低レベルフォーマット
送信宛先データファイル	E-mail アドレスや電話番号などの宛先データはすべて削除される。	SSD 低レベルフォーマット
管理者パスワード	現在設定されているパスワードをクリアし、出荷時設定に戻します。	全設定初期化
SNMP パスワード	現在設定されているパスワードをクリアし、出荷時設定（MAC アドレス）に戻します。	全設定初期化
SSL 証明書	現在設定されている SSL 証明書が削除される。	全領域上書き削除 SSD 低レベルフォーマット 全設定初期化
ネットワーク設定	現在設定されているネットワーク設定（DNS サーバー、IP アドレス、SMTP サーバー、NetWare 設定、NetBIOS 設定、Apple-Talk プリンタ名設定）をクリアし、出荷時設定に戻します。	全設定初期化
本機の設定データ	本機の設定データが削除される。	全設定初期化

クリアされる項目	クリア内容	クリア方法
高信頼チャネルの設定データ	高信頼チャネルの設定データが削除される。	全設定初期化
外部サーバー識別の設定データ	外部サーバー識別の設定データが削除される。	全領域上書き削除

HDD フォーマットについて

HDD フォーマットは HDD を初期化（出荷時状態に戻す）したい場合や、HDD を交換した場合などに行います。HDD フォーマットを行うと、本機 HDD 内に保存されているデータが削除されます。フォーマットの種類により削除されるデータが異なります。

- ［ユーザーエリア（プリント)］を行うと、機密印刷ファイル、認証＆プリントファイルが削除されます。
- ［ユーザーエリア（スキャン)］を行うと、登録ユーザー情報および HDD 送信ファイルが削除されます。
- ［全領域］を行うと、HDD 内の全領域がフォーマットされ、保存されている全データが削除されます。またフォーマットによりセキュリティ強化設定が［しない］に設定されます。再度［する］に設定してください。設定方法について詳しくは、2-5 ページをごらんください。

ファームウェアの書き換えについて

サービスエンジニアによってファームウェアの書き換えが行われた場合、本機管理者による［全設定初期化］の実行が必要です。ファームウェアの書き換え後に、［全設定初期化］を実行してください。［全設定初期化］の実行について詳しくは、2-26 ページをごらんください。

- ［全設定初期化］によりクリアされる項目について詳しくは、1-10 ページをごらんください。
- ［全設定初期化］の実行により、セキュリティ強化設定が［しない］に設定されます。再度［する］に設定してください。設定方法について詳しくは、2-5 ページをごらんください。

2 管理者編

2 管理者編

2.1 管理者設定にアクセスする

本機は、管理者設定の機能を使用するために、アクセスする者が管理者であることを 8 桁の管理者パスワードを使用して認証します。認証中、入力されたパスワードは、「*」または「●」として表示されます。パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。

重要
管理者パスワードは絶対に一般ユーザーには知られないようにしてください。

管理者パスワードを忘れた場合、サービスエンジニアによる設定が必要です。サービス実施店にご連絡ください。

管理者設定へのアクセスのしかた

以下の場合、管理者設定へのアクセスを受け付けません。しばらく待ったのち、再度管理者設定へのアクセスを行ってください。

- 本機で実行中のジョブがある場合
- 本機内にジョブ予約（タイマー送信、Fax リダイヤル待ちなど）がされている場合
- 電源スイッチが ON された直後の場合
- 本機でトラブルコードが表示されている場合

＜操作パネルからのアクセス＞

✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

1 ［設定メニュー / カウンター］を押します。

2 ［↓］を押します。

3 ［管理者設定］を押します。



4 キーボードまたはテンキーで 8 桁の管理者パスワードを入力します。



➔ [C] を押すと、入力された値がクリアされます。
➔ [削除] を押すと、入力した文字が 1 文字ずつ削除されます。
➔ [↑] を押すと、大文字画面に切り替わります。
➔ [!#?/] を押すと、記号画面に切り替わります。

5 [OK] を押します。

➔ 管理者パスワードを間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しい管理者パスワードを入力してください。
➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

6 [リセット] を押すと、管理者設定をログアウトします。

＜PageScope Web Connection からのアクセス＞

✔ ジョブ実行中管理者モードにログインしようとした場合、管理者モードにログインできないことを告げるメッセージが表示されます。［OK］をクリックし、ジョブ終了後、再度管理者モードにログインしてください。

✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 Web ブラウザを起動します。

2 アドレスバーに本機の IP アドレスを入力します。

3 ［Enter］を押し、PageScope Web Connection を起動します。

4 管理者のラジオボタンをクリックし、［ログイン］をクリックします。



5 パスワードボックスに、8 桁の管理者パスワードを入力します。



➔ PageScope Web Connection を使用して管理者モードにアクセスする場合は、本機と同じ管理者パスワードを入力してください。

6 ［OK］をクリックします。

➔ 管理者パスワードを間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しい管理者パスワードを入力してください。

➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

7 ［ログアウト］をクリックすると、管理者モードをログアウトします。

2.2 セキュリティー機能を強化する

本機は、操作パネルから管理者設定によって本機管理者が認証されると、各セキュリティー機能を強化するための設定を一括で変換する、セキュリティ強化設定の動作設定を許可します。

セキュリティ強化設定では、セキュリティ強化設定を利用するか利用しないかの選択が可能です。セキュリティ強化設定を［する］にした場合、各種パスワードが一定の基準を満たしているかなどの機能を自動的に設定し、セキュリティー機能を強化します。

セキュリティ強化設定を［する］に設定するには、以下の設定をあらかじめ行う必要があります。

あらかじめ必要な設定	設定内容
管理者パスワード	8 桁のパスワードでパスワード規約の条件を満たす 出荷時設定では「12345678」が設定されています
ユーザー認証	［デバイス］または［外部サーバー］（Active Directory）に設定する
SSL 証明書	SSL 通信を行うため、自己証明書の登録を行う
パスワード規約	［する］に設定する

セキュリティ強化設定を［する］に設定した場合、以下の機能の設定値が変更されます。

機能名	出荷時設定	セキュリティ強化設定有効時
パブリック許可	制限	制限 (変更不可)
認証なしプリント	制限	制限 (変更不可)
ユーザーリスト表示設定	しない	しない (変更不可)
SSL	無効	有効 (変更不可)
SSL 暗号化強度	AES-256, 3DES, RC4-128, DES, RC4-40	AES-256, 3DES (AES/3DES より低い強度が含まれる設定に変更不可)
FTP サーバー	有効	有効 / 無効の切り替え可
SNMPv1/v2c	リード / ライト有効	リードのみ許可（変更不可）
SNMP v3 Security Level および auth/priv-password（SNMP v3 ライトユーザー）	auth-password /priv-password	Security Level を［auth-password］または［auth-password/priv-password］から選択可能 8 桁以上の auth-password または auth/priv-password の両パスワードを設定可能
ネットワーク経由の管理者パスワード変更 (Pagescope Web Connection)	許可	禁止
ネットワーク経由でのファームウェア書き換え制限	無効	有効
CS Remote Care	使用可能	リモートでのデバイス設定不可
Telnet	有効	無効 (変更不可)

重要

パスワード規約が［する］に設定されると、それぞれのパスワードに使用できるキャラクタおよび桁数が制限されます。パスワード規約について詳しくは、1-8 ページをごらんください。

セキュリティ強化設定を［する］にしても、認証＆プリント機能は有効になりません。画像ファイルを保護するため、手動で設定を有効にしてください。認証＆プリント機能について詳しくは、2-12 ページをごらんください。

本機管理者が以下のいずれかの設定を行うと、セキュリティ強化設定が［しない］に設定されます。セキュリティ強化設定を再度［する］に設定してください。

- ［HDD フォーマット］の［全領域］を実行した場合
- ［全領域上書き削除］を実行した場合
- ［SSD 低レベルフォーマット］を実行した場合
- ［全設定初期化］を実行した場合
- ［ネットワーク設定初期化］を実行した場合
- ［システム設定初期化］を実行した場合

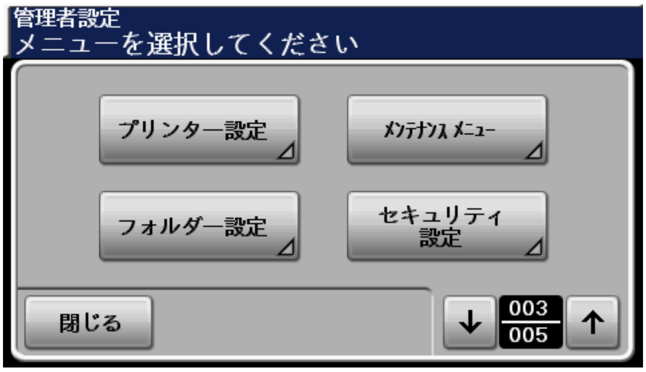
セキュリティ強化設定の設定のしかた

✔ 管理者設定の表示のしかたは、2-2 ページをごらんください。
✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。
✔ セキュリティ強化設定の出荷時設定は［しない］が設定されています。本機のセキュリティー機能を有効にするために、必ず［する］に設定してください。

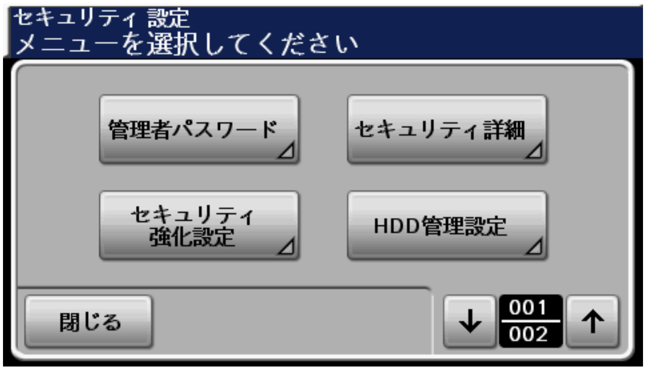
1 操作パネルより管理者設定を表示させせます。

2 ［↓］を押します。

3 ［セキュリティ設定］を押します。



4 ［セキュリティ強化設定］を押します。



5 セキュリティ強化設定を有効にする場合は、［する］を選択し、［OK］を押します。
［OK］を押すと、自動で本機が再起動を行います。



➔ 本機管理者によって、あらかじめ必要な設定がされていない場合、[する]を選択することができません。必要な設定について詳しくは、2-5 ページをごらんください。
2-5 ページ

➔ 正しくセキュリティ強化設定が行われると、画面の赤枠部分に鍵マークのアイコンが表示され、セキュリティ強化設定中であることを示します。



2.3　認証方式を設定する

本機は、管理者設定によって本機管理者が認証されると、ユーザー認証を行うときの認証方式の設定操作を許可します。

ユーザー認証の認証方式には、本機自身の認証システムを利用する［デバイス］、外部サーバーの持つユーザー情報管理システムを利用して認証を行う［外部サーバー］また［オフ］の 3 種類があります。セキュリティ強化設定を［する］に設定する場合、認証方式を［デバイス］か［外部サーバー］（Active Directory）での運用を行ってください。

また［デバイス］を選択した場合は、IC カード機能を設定できます。IC カード機能とは、本機に接続した IC カードリーダーで IC カードを読み取り、ユーザー認証を行います。

重要
認証方式で［外部サーバー］を選択した場合、外部サーバー設定において必ず［Active Directory］を選択してください。

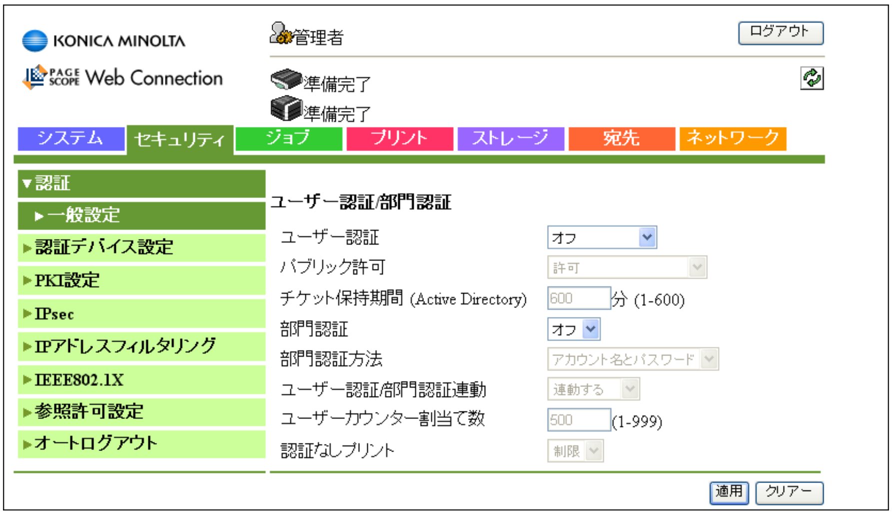
認証方式の設定のしかた

✔　管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

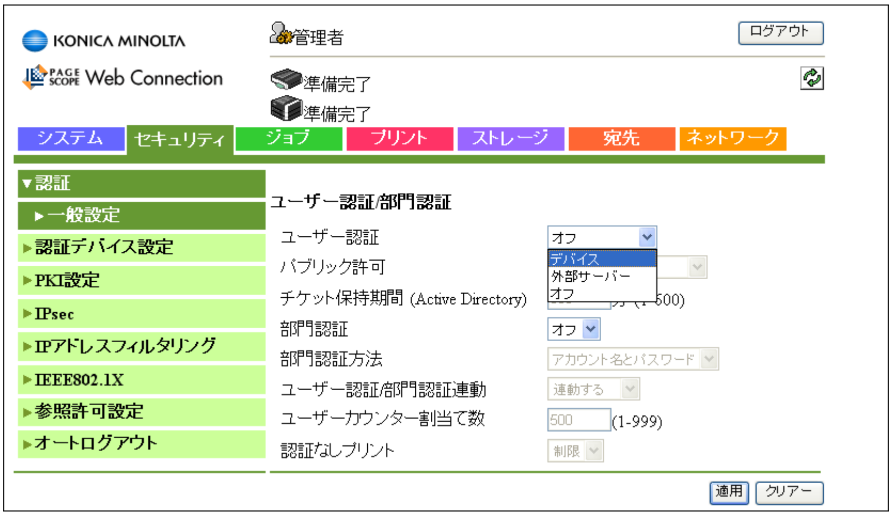
✔　管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1　PageScope Web Connection を起動し、管理者モードにアクセスします。

2　［セキュリティ］タブをクリックします。



3　ユーザー認証のプルダウンメニューより、［デバイス］または［外部サーバー］を選択します。
［デバイス］を選択した場合は手順 4 ～ 5 を行ってください。
［外部サーバー］を選択した場合は手順 6 ～ 10 を行ってください。



4 ［デバイス］を選択した場合は、［認証デバイス設定］メニューより［一般設定］をクリックし、［認証タイプ］および［IC カードタイプ］を設定します。



認証方式	内容
なし	ユーザー認証に IC カードを使用しません。ユーザー名とユーザーパスワードを入力して認証する方式です。
カード認証	ユーザー名とユーザーパスワードを入力する認証のほかに、IC カードを使用して識別する方式です。
カード認証 + パスワード	ユーザー名とユーザーパスワードを入力する認証のほかに、IC カードを IC カードリーダーに置いたあと、ユーザーパスワードを入力して認証する方式です。

➔ IC カード機能を利用するには、ユーザーの IC カード情報を本機に登録する必要があります。詳しくは 2-18 ページをご覧ください。

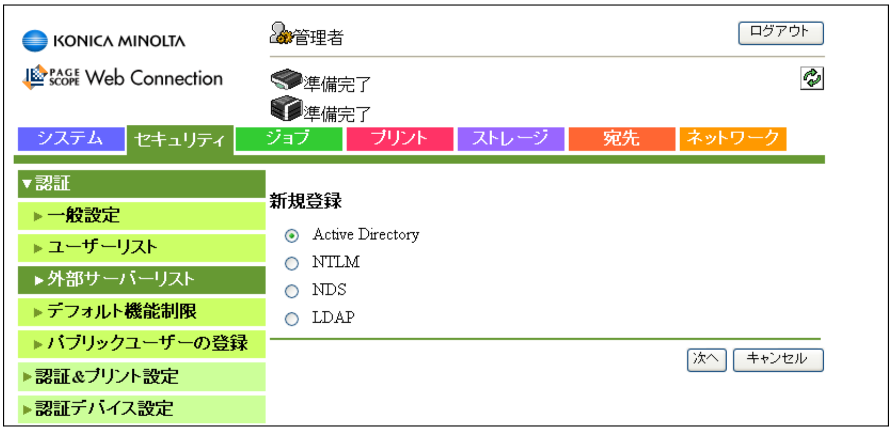
5 ［適用］をクリックします。

6 ［外部サーバー］を選択した場合は、［認証］メニューより［外部サーバーリスト］をクリックします。

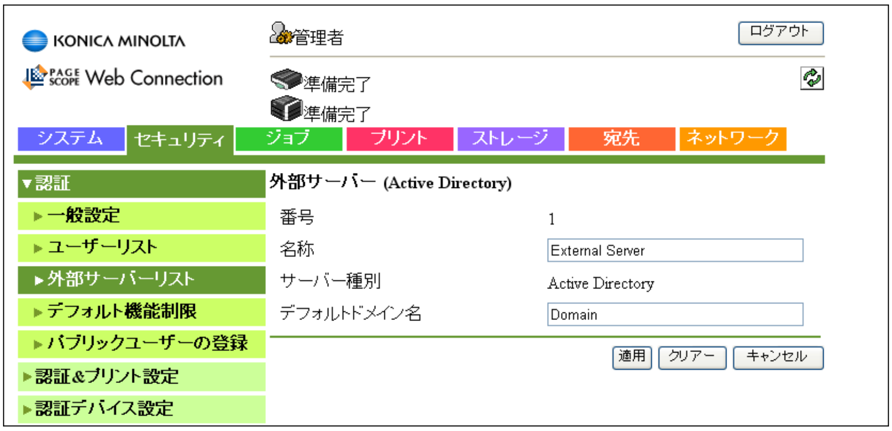
7 ［編集］をクリックします。



8 ［Active Directory］を選択して、［次へ］をクリックします。



9 各種設定を行います。



10 ［適用］をクリックします。

2.4　認証＆プリント設定機能

本機は、管理者設定によって本機管理者が認証されると、認証＆プリント機能の動作設定を許可します。

認証＆プリント機能とは、PC から送信した印刷データをいったん本機の HDD に蓄積しておき、本機でのユーザー認証が成功したあと、該当ユーザーの印刷データを自動的に印刷する機能です。

重要
認証＆プリント機能を設定するには、あらかじめ管理者によるユーザー認証の設定が必要です。ユーザー認証について詳しくは 2-9 ページをごらんください。

認証＆プリント設定のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。
✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1　PageScope Web Connection を起動し、管理者モードにアクセスします。

2　［セキュリティ］タブをクリックし、［認証＆プリント設定］をクリックします。

3　［認証＆プリント］のプルダウンメニューから、［有効］を選択します。



➔［有効］を設定すると、プリンタードライバー側で［印刷］を選択した場合でも、認証＆プリントファイルとして保存されます。
➔［無効］を設定していても、プリンタードライバー側で［認証＆プリント］を選択した場合は、認証＆プリントファイルとして保存されます。

4　［適用］をクリックします。

2.5　オートリセット機能

本機は、操作パネルから管理者設定によって本機管理者が認証されると、オートリセット機能の動作設定を許可します。

オートリセット機能は、操作パネルから管理者設定およびユーザーモード（ユーザー認証設定時）へのアクセス中、何も操作が行われない状態が設定時間に達すると、自動的に各モードをログアウトします。

オートリセット機能がはたらくまでの時間は、1 分～ 9 分または［しない］から設定できます。オートリセット機能を［しない］に設定した場合でも、1 分間何も操作が行われなかった場合、自動的に各モードをログアウトします。

参考

- 操作処理中の無操作状態が設定時間に達した場合でも、ジョブ処理動作を優先するため、自動的に各モードをログアウトすることはありません。ジョブ処理終了後から設定時間経過でログアウトします。

オートリセット機能の設定のしかた

✔ 管理者設定の表示のしかたは、2-2 ページをごらんください。

✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

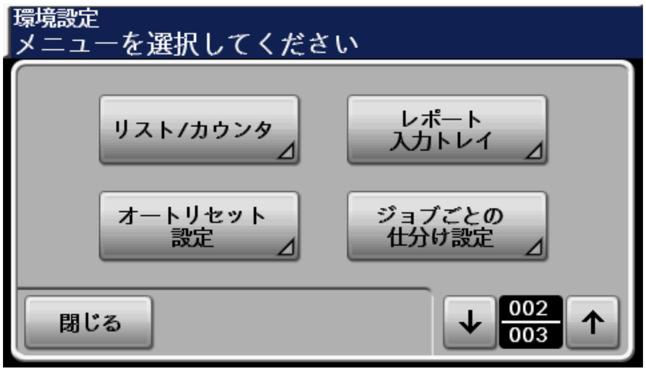
1 操作パネルより管理者設定を表示させます。

2 ［環境設定］を押します。

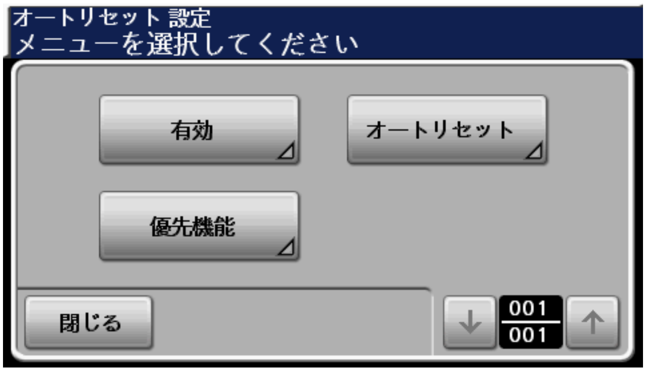


3 ［↓］を押します。

4 ［オートリセット設定］を押します。



5 ［有効］を押します。

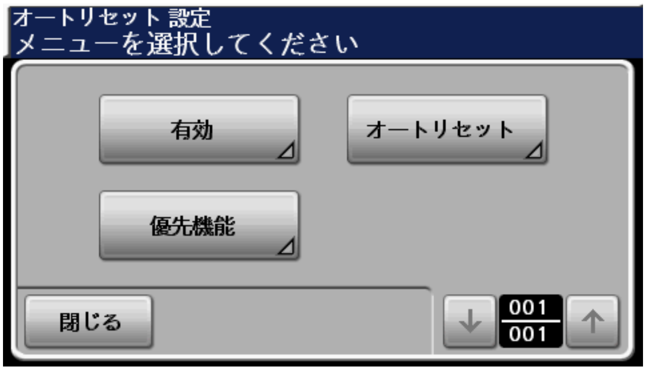


6 ［する］を選択し、［OK］を押します。



➔ ［しない］を選択した場合でも、1 分間何も操作が行われなければオートリセット機能がはたらき自動的にログアウトします。

7 ［オートリセット］を押します。



8 オートリセットがはたらくまでの時間（1 分～ 9 分）を［-］/［+］で入力します。



➔ オートリセットは、1 分～ 9 分の間で 1 分単位の設定が行えます。

9 ［OK］を押します。

2.6 ユーザー設定機能

本機は、管理者設定によって本機管理者が認証されると、本機を使用できるユーザーの登録を許可します。また、ユーザーの削除およびユーザーパスワード変更操作を許可します。

ユーザー登録とは、本機へのアクセスまたは操作を許可するため、ユーザー名およびユーザーパスワードなどのユーザー情報を登録する機能です。ユーザーは最大 1,000 件まで登録できます。ユーザー登録することで、各ユーザーを識別認証し、本機の不正使用を防止します。ユーザーパスワードは、8 桁以上 64 桁までのパスワードで管理され、入力されたパスワードは、「＊」または「●」として表示されます。

参考

- 認証方式で［外部サーバー］（Active Directory）が設定されている場合、PageScope Web Connection からユーザー登録およびユーザーパスワード変更操作はできません。ユーザーの登録および変更を行う場合は、サーバー側での設定を行ってください。ただし、PageScope Data Administrator を利用してユーザー情報を登録する場合、ユーザー名は外部サーバーに登録されているユーザー名と一致していなければなりません。また、ユーザーパスワードの設定は可能ですが、認証には使用されません。
- 認証方式にて［外部サーバー］（Active Directory）が設定されている場合、本機に登録されていないユーザーがユーザー認証にて認証されるとユーザー名は自動的に本機に登録されます。
- 認証方式にて［外部サーバー］（Active Directory）が設定されている場合、本機に登録されているユーザーがユーザー認証にて認証されると、同じユーザー名称で外部サーバー名称とともに自動的に本機に登録されます。ただし、外部サーバー内で同じユーザー名を登録することはできません。
- 認証方式にて［デバイス］と［外部サーバー］の間でユーザー認証方式をそれぞれ変更した場合は、変更前の認証方式に登録されていたユーザー情報は、変更後の認証方式では使用できません。変更後にユーザー情報を再度設定してください。
- 認証方式にて［外部サーバー］（Active Directory）が設定されている場合、外部サーバー側でユーザー名を変更する場合は、変更するユーザーを本体から削除したあと行ってください。
- 認証方式にて［デバイス］が設定されている場合、ユーザー名を変更すると変更前のユーザーが所有していた画像ファイルは削除されます。
- 複数の外部サーバーを使用して認証を行う場合は、各サーバーに登録するユーザー名が同一となるよう管理を行ってください。
- 認証方式にて［外部サーバー］(Active Directory) が設定されている場合、外部サーバーを削除するとサーバーに関連する以下のユーザー登録情報およびデータが削除されます。
- ユーザー名、ユーザーパスワード
- ユーザーが所有していた HDD 送信ファイル、機密印刷ファイル、認証＆プリントファイル

ユーザー設定のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

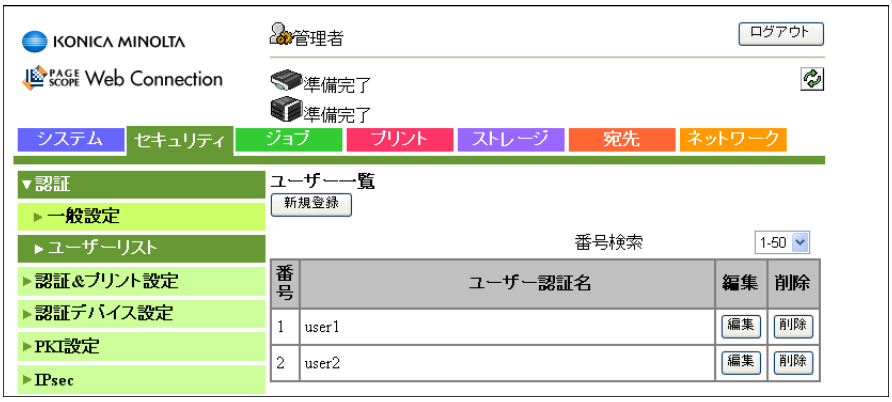
✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

✔ ユーザーを登録した場合は、速やかに該当するユーザーに通知するとともに、ユーザー自身によってパスワードの変更を行わせてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

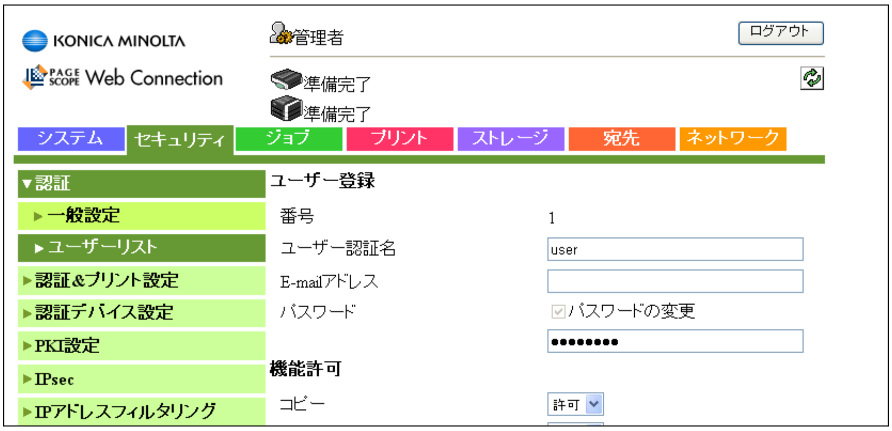
2 ［セキュリティ］タブをクリックし、［ユーザーリスト］をクリックします。

3 ［新規登録］をクリックします。



➔ ユーザーパスワードを変更する場合は、［編集］をクリックし、「パスワードの変更」のチェックボックスをクリックし、新しいユーザーパスワードを入力してください。

4 各種設定を行います。



➔ 既に登録済みのユーザー名と同一のユーザー名を重複して登録することはできません。
➔ ［キャンセル］をクリックすると、前の画面に戻ります。

5 ［適用］をクリックします。

➔ 入力したユーザーパスワードがパスワード規約の条件を満たしていない場合、入力したユーザーパスワードは使用できないことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。パスワード規約について詳しくは、1-8 ページをごらんください。

6 設定が完了したことを告げるメッセージを確認し、［OK］をクリックします。

➔ 登録済みのユーザーを削除する場合は、手順 3 で［削除］をクリックします。確認画面で登録内容を確認し、削除する場合は、［OK］をクリックします。ユーザーを削除した場合、削除したユーザーの所有する画像ファイルは削除されます。

2.7　IC カード情報設定機能

本機は、管理者設定によって本機管理者が認証されると、IC カード情報の設定操作を許可します。

本機ではユーザー名とユーザーパスワードを入力する認証のほかに、IC カードを使用した認証ができます。IC カード機能を使用するためには、ユーザーの IC カード情報を本機に登録する必要があります。登録されたユーザーは IC カードを使用してユーザー認証を行い、本機へログインできます。

IC カード情報の登録には 2 つの方法があります。
- IC カードリーダーを本機に接続し、直接本機に登録する
- IC カードリーダーを管理者の PC に接続し、PageScope Data Administrator を使用して登録する

PageScope Data Administrator を使用して登録する方法について詳しくは 4-10 ページをご覧ください。

重要
IC カード情報を登録するには、あらかじめ管理者によるユーザー認証および認証デバイスの設定が必要です。ユーザー認証および認証デバイスの設定について詳しくは 2-9 ページをごらんください。

操作パネルからの登録のしかた

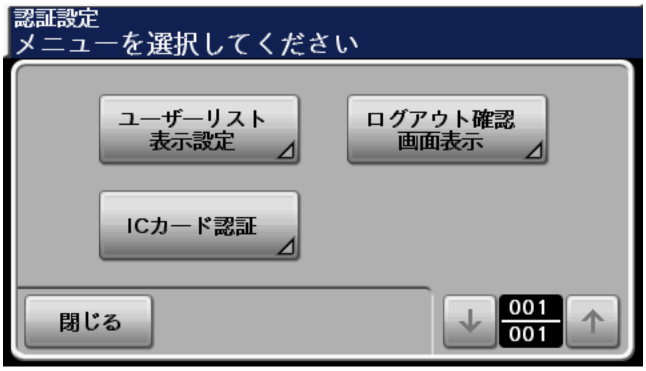
✔　管理者設定の表示のしかたは、2-2 ページをごらんください。
✔　管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

1　操作パネルより管理者設定を表示させます。

2　［認証設定］を押します。



3　［IC カード認証］を押します。



4 登録するユーザー名を選択して、[OK] を押します。



➔ [すべて] を押すと、全ユーザーが表示されます。[検索] を押すと、ユーザーを検索できます。

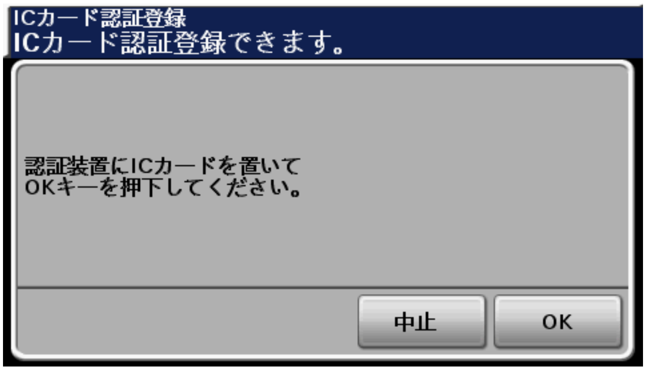
5 [編集] を押します。



➔ 登録済みの IC カード情報を変更する場合、および PageScope Data Administrator の [カード ID の直接入力] からカード ID の登録をした場合も、[編集] を押します。

➔ 登録済みの IC カード情報を削除する場合は、[削除] を押します。確認画面が表示されますので、[はい] を選択して [OK] を押します。

6 IC カードリーダーに IC カードを置き、[OK] を押します。



7 [閉じる] を押します。

2.8 管理者パスワードを変更する

本機は、操作パネルから管理者設定によって本機管理者が認証されると、管理者設定へアクセスするための管理者パスワードの変更操作を許可します。

入力された管理者パスワードは、「＊」として表示されます。

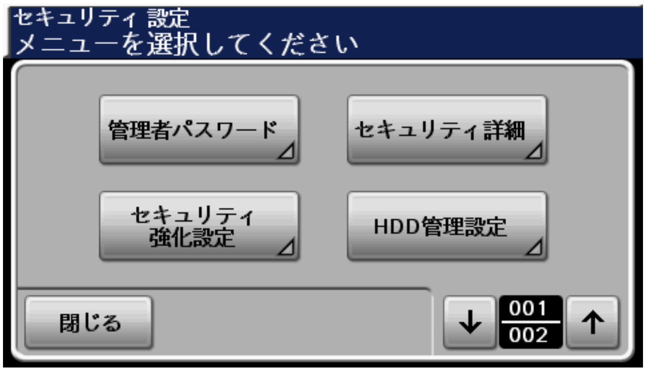
管理者パスワードの変更のしかた

✔ セキュリティ設定画面の表示のしかたは、2-7 ページの手順 1 ～ 3 をごらんください。

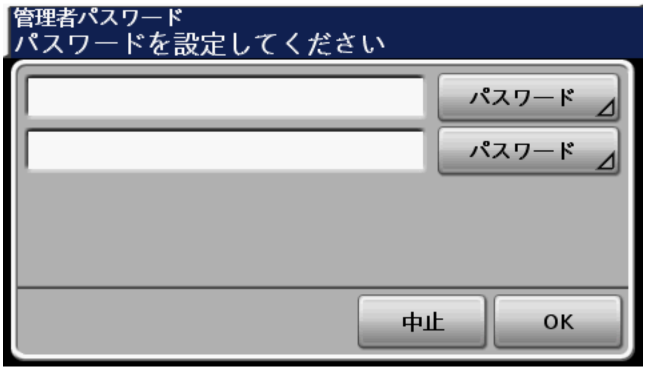
✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

1 操作パネルよりセキュリティ設定画面を表示させます。

2 ［管理者パスワード］を押します。



3 上段の［パスワード］を押します。



4 キーボードまたはテンキーで新しい 8 桁の管理者パスワードを入力します。

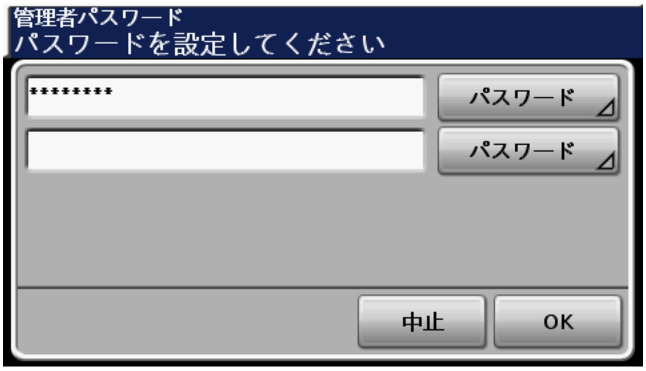


➔ ［C］を押すと、入力された値がクリアされます。
➔ ［削除］を押すと、入力した文字が 1 文字ずつ削除されます。
➔ ［↑］を押すと、大文字画面に切り替わります。

➔ ［!#?/］を押すと、記号画面に切り替わります。

5 ［OK］を押します。

6 下段の［パスワード］を押します。

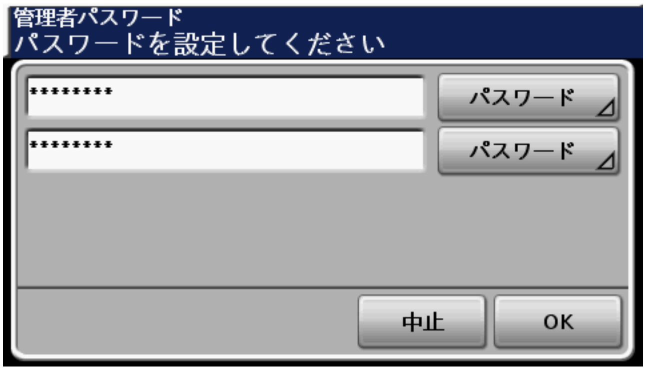


7 誤入力防止のため 8 桁の管理者パスワードを再度入力します。



➔ ［C］を押すと、入力された値がクリアされます。
➔ ［削除］を押すと、入力した文字が 1 文字ずつ削除されます。
➔ ［↑］を押すと、大文字画面に切り替わります。
➔ ［!#?/］を押すと、記号画面に切り替わります。

8 ［OK］を押します。



➔ 入力した管理者パスワードがパスワード規約の条件を満たしていない場合、入力した管理者パスワードは使用できないことを告げるメッセージが表示されます。正しい管理者パスワードを入力してください。パスワード規約について詳しくは、1-8 ページをごらんください。
➔ 入力した管理者パスワードが一致していない場合、管理者パスワードが一致していないことを告げるメッセージが表示されます。正しい管理者パスワードを入力してください。

2.9　廃棄またはリース返却時のデータ消去について

本機は、操作パネルから管理者設定によって本機管理者が認証されると、全領域上書き削除、SSD 低レベルフォーマット、全設定初期化の動作設定を許可します。

本機を廃棄またはリース返却する場合、本機に残存するデータの漏洩を防止するため、データ消去を行ってください。データ領域によってデータ消去の方法が異なります。詳しくは、下表をごらんください。

データ領域	消去方法
HDD	全領域上書き削除
SSD	SSD 低レベルフォーマット
NVRAM	全設定初期化

重要
データ消去は HDD、SSD、NVRAM すべて行ってください。

データ消去を行う際は、すべてのデータ消去が正常に完了したことを確認してください。データ消去実行中にエラーが発生した場合はサービス実施店にお問い合わせください。

全領域上書き削除、SSD 低レベルフォーマット、全設定初期化のいずれかを実行すると、セキュリティ強化設定が［しない］に設定されます。

2.9.1　全領域上書き削除の設定のしかた

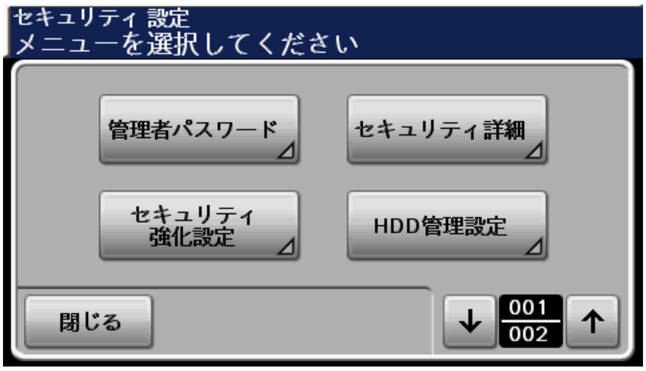
上書き消去方式は［モード 1］～［モード 8］の 8 つのモードのいずれかから選択できます。全データ上書き消去に要する時間は、最小の［モード 1］で約 1 時間弱、最大の［モード 8］で約 9 時間程度を必要とします。

モード	説明
モード 1	「0x00」で 1 回上書きします。
モード 2	「乱数」▸▸「乱数」▸▸「0x00」で上書きします。
モード 3	「0x00」▸▸「0xff」▸▸「乱数」で上書き ▸▸ 検証します。
モード 4	「乱数」▸▸「0x00」▸▸「0xff」で上書きします。
モード 5	「0x00」▸▸「0xff」▸▸「0x00」▸▸「0xff」で上書きします。
モード 6	「0x00」▸▸「0xff」▸▸「0x00」▸▸「0xff」▸▸「0x00」▸▸「0xff」▸▸「乱数」で上書きします。
モード 7	「0x00」▸▸「0xff」▸▸「0x00」▸▸「0xff」▸▸「0x00」▸▸「0xff」▸▸「0xaa」で上書きします。
モード 8	「0x00」▸▸「0xff」▸▸「0x00」▸▸「0xff」▸▸「0x00」▸▸「0xff」▸▸「0xaa」で上書き ▸▸ 検証します。

✔ セキュリティ設定画面の表示のしかたは、2-7 ページの手順 1 ～ 3 をごらんください。
✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。
✔ クリアされる項目について詳しくは、1-10 ページをごらんください。

1 操作パネルよりセキュリティ設定画面を表示させます。

2 ［HDD 管理設定］を押します。



3 ［全領域上書き削除］を押します。



4 ［モード］を押します。



5 目的のモードを選択します。

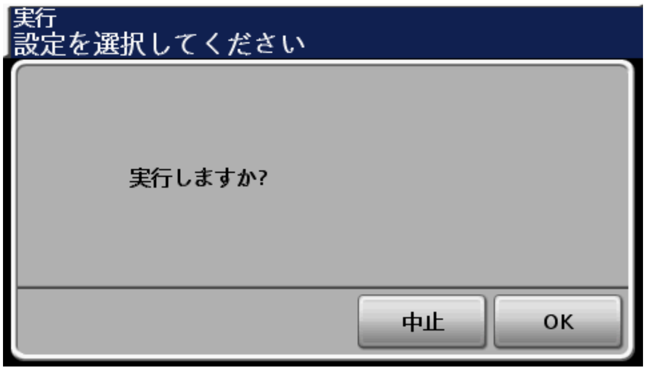


6 ［OK］を押します。

7 ［実行］を押します。



8 確認メッセージが表示されます。［OK］を押します。



➔ 全領域上書き削除実行中は、本機電源スイッチを OFF にしないでください。実行中に誤って電源スイッチを OFF にして、本機が HDD を認識しないなどの不具合が発生した場合はサービス実施店にお問い合わせください。

2.9.2 SSD 低レベルフォーマットの設定のしかた

SSD のデータ領域に対して、固定値（0x00）で上書き消去を行います。

✔ セキュリティ設定画面の表示のしかたは、2-7 ページの手順 1 ～ 3 をごらんください。
✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。
✔ クリアされる項目について詳しくは、1-10 ページをごらんください。

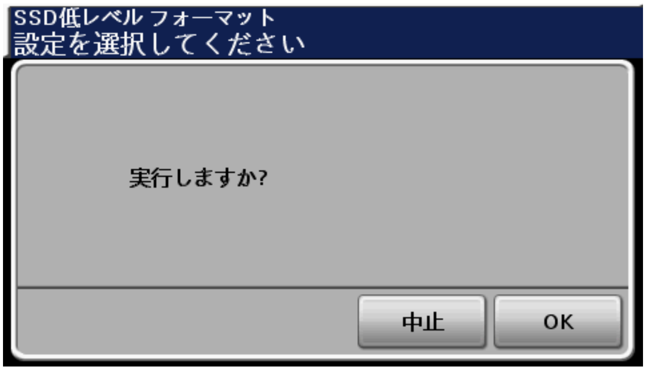
1 操作パネルよりセキュリティ設定画面を表示させます。

2 ［↓］を押します。

3 ［SSD 低レベルフォーマット］を押します。



4 確認メッセージが表示されます。［OK］を押します。



➔ SSD 低レベルフォーマット中は、本機電源スイッチを OFF にしないでください。実行中に誤って電源スイッチを OFF にして、不具合が発生した場合はサービス実施店にお問い合わせください。

2.9.3 全設定初期化の設定のしかた

NVRAM を初期化し、出荷時状態に戻します。

✔ 管理者設定の表示のしかたは、2-2 ページをごらんください。
✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。
✔ クリアされる項目について詳しくは、1-10 ページをごらんください。

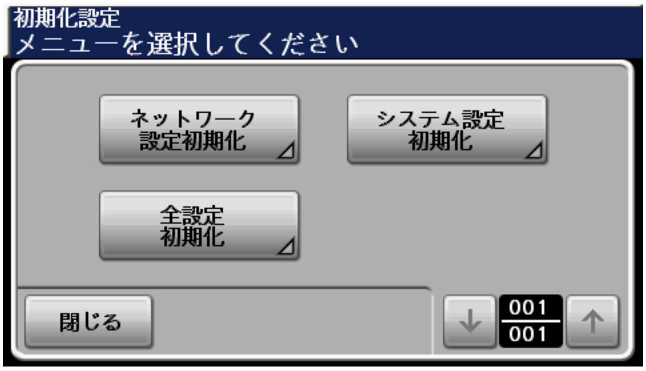
1 操作パネルより管理者設定を表示させせます。

2 ［↓］を押します。

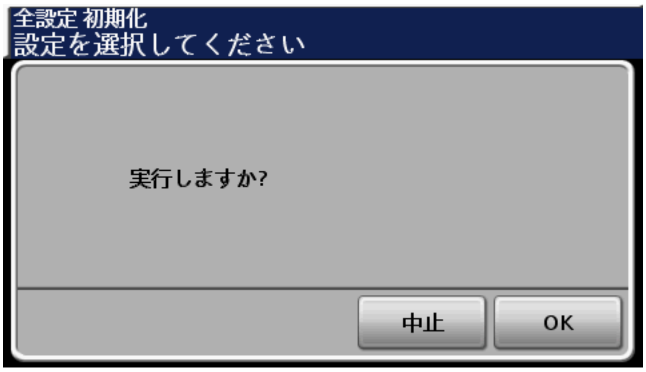
3 ［初期化設定］を押します。



4 ［全設定初期化］を押します。



5 確認メッセージが表示されます。［OK］を押します。



➔ 全設定初期化実行中は、本機電源スイッチを OFF にしないでください。実行中に誤って電源スイッチを OFF にして、不具合が発生した場合はサービス実施店にお問い合わせください。

2.10 SSL 設定機能

本機は、管理者設定によって本機管理者が認証されると、PC と本機間で送受信される画像データの暗号化設定を許可します。

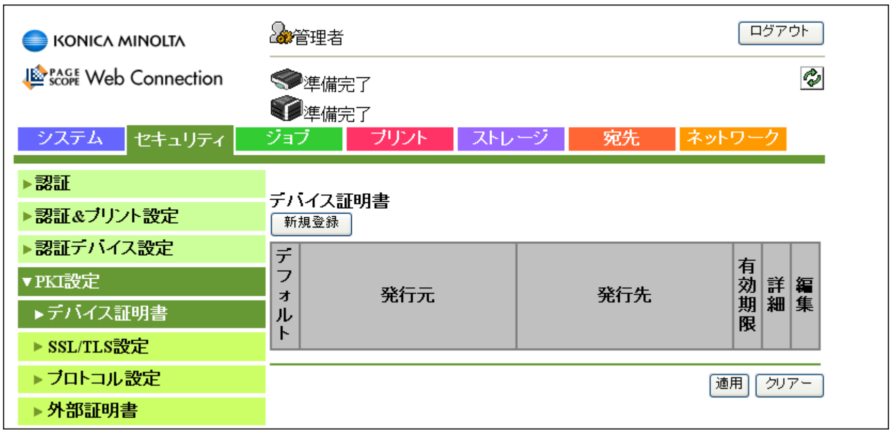
2.10.1 デバイス証明書設定のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。
✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。
✔ SSL 証明書設定において生成されるサーバーの公開鍵の鍵長は 1024bit が設定されます。
✔ セキュリティ強化設定中に証明書の有効期限が切れても、セキュリティ強化設定は［しない］になりません。本機管理者は証明書の有効期限が切れる前に、新しい証明書の登録を行ってください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［セキュリティ］タブをクリックし、［PKI 設定］をクリックします。

3 ［新規登録］をクリックします。



4 ［証明書の自己作成］を選択し、［次へ］をクリックします。



5 各種設定を行います。



→ 各項目の入力が条件を満たさずに［適用］をクリックすると、内容がすべてクリアされます。

6 ［適用］をクリックします。

証明書が登録できます。

2.10.2 SSL 使用設定のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

重要

SSL の使用設定をするには、必ず事前にデバイス証明書が本機に登録されていることを確認してください。デバイス証明書の登録について詳しくは、2-27 ページをごらんください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［セキュリティ］タブをクリックし、［PKI 設定］の［SSL/TLS 設定］をクリックします。

3 暗号強度を設定し、［適用］をクリックします。



➔ 暗号強度は強度の高い「AES-256, 3DES」を選択してください。

➔ セキュリティ強化設定中は AES/3DES より低い強度が含まれる設定には変更できません。

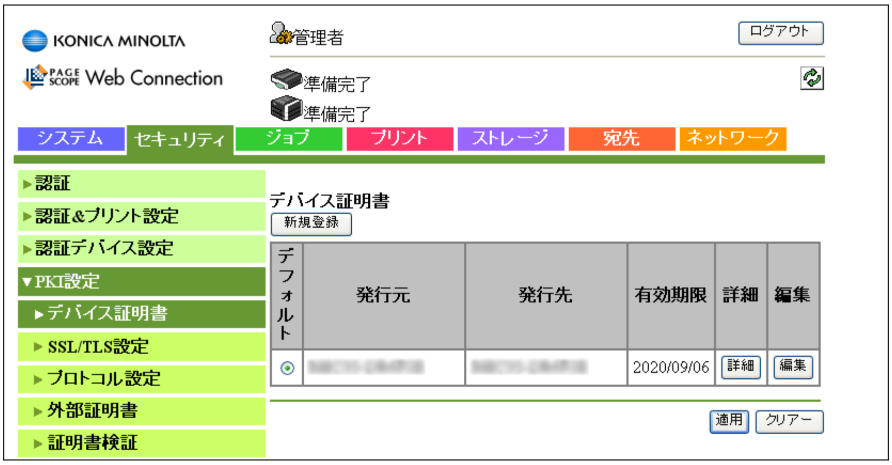
2.10.3 証明書の破棄のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。
✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。
✔ セキュリティ強化設定中は、証明書の破棄はできません。

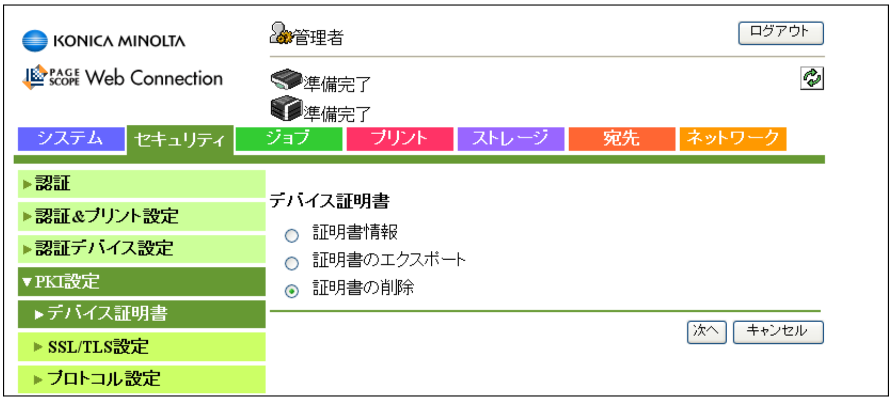
1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［セキュリティ］タブをクリックし、［PKI 設定］をクリックします。

3 ［編集］をクリックします。



4 ［証明書の削除］を選択し、［次へ］をクリックします。



5 ［OK］をクリックします。



2.11 SNMP 設定機能

本機は、管理者設定によって本機管理者が認証されると、PC から SNMP を利用してネットワークを介し MIB オブジェクトへアクセスするための SNMP v3 Write User パスワード（auth-password、priv-password）の変更を許可します。

auth-password および priv-password には、それぞれ 8 桁～ 32 桁のパスワードが設定できます。入力されたパスワードは、「●」として表示されます。

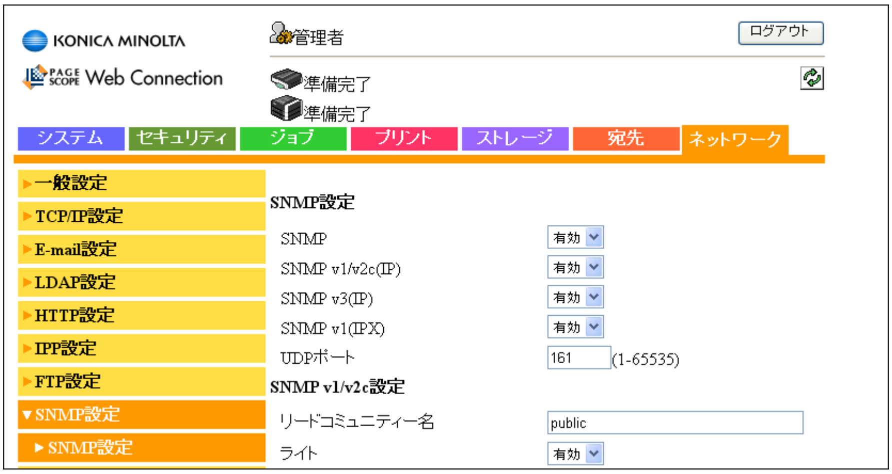
2.11.1 auth-password および priv-password の変更のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ネットワーク］タブをクリックし、［SNMP 設定］をクリックします。



3 ［パスワードの変更］のチェックボックスをクリックし、SNMP v3 設定枠部（ライト側）の auth-password および priv-password を入力します。



➔ auth-password および priv-password の出荷時設定値は、本機に設定されている MAC アドレスです。

4 ［適用］をクリックします。

➔ 入力した auth-password または priv-password がパスワード規約の条件を満たしていない場合、内容がクリアされます。正しい auth-password または priv-password を入力してください。パスワード規約について詳しくは、1-8 ページをごらんください。

2.11.2 SNMP アクセス認証機能

PC より SNMP を利用して管理者モードの設定を変更する場合、本機で設定された SNMP v3 Write 設定の Write User Name と SNMP パスワード（auth-password、priv-password）により、アクセスする利用者が管理者であることを認証します。

Write User Name に対して SNMP パスワードが一致した管理者に対し SNMP を利用したネットワークを介して利用することができるセキュリティー管理機能のネットワーク設定機能、SNMP パスワード変更機能の操作を許可します。

参考

- Security Level の［auth-password］を選択していた場合、通信される認証情報（auth-password）はハッシュ化されます。本機の場合ハッシュには HMAC-MD5 または HMAC-SHA1 から選択することができます。
- また、Security Level の［auth-password/priv-password］を選択していた場合、通信される認証情報（auth-password/priv-password）やデータ（変更対象を指定するオブジェクト ID やセットされる値など）はハッシュ、暗号化に利用されます。本機の場合暗号化には CBC-DES または CBC-AES から選択することができます。
- MIB へのアクセスには、上記の暗号アルゴリズムに対応した MIB ブラウザをご利用ください。

2.11.3 SNMP v3 設定機能

PC より SNMP アクセス認証にて認証された管理者は、SNMP パスワード変更機能の操作を許可します。

auth-password、priv-password にはパスワード規約の条件を満たしたパスワードを入力してください。パスワード規約について詳しくは、1-8 ページをごらんください。

設定を変更する場合、オブジェクト ID にて指定してください。設定項目については下表をごらんください。

設定項目	オブジェクト ID
Write User Name	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.2.2
auth-password	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.3.2
priv-password	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.4.2
Security Level	1.3.6.1.4.1.18334.1.1.2.1.5.6.4.2.1.5.2

2.11.4 SNMP ネットワーク設定機能

PC より SNMP アクセス認証にて認証された管理者は、ネットワーク設定機能の操作を許可します。設定を変更する場合、オブジェクト ID にて指定してください。設定項目については下表をごらんください。

設定項目		オブジェクト ID
IP アドレス設定	IP アドレス	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.3.1
	BOOT プロトコル使用設定	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.6.1
	BOOT プロトコルタイプ	1.3.6.1.4.1.18334.1.1.2.1.5.7.1.1.1.7.1
DNS サーバーアドレス設定		1.3.6.1.4.1.18334.1.1.2.1.5.7.1.2.1.3.1.1
SMTP サーバーアドレス設定		1.3.6.1.4.1.18334.1.1.2.1.5.7.13.1.1.3.1
NetWare 設定	プリントサーバー名	1.3.6.1.4.1.18334.1.1.2.1.5.8.3.1.3.1.1
	プリンタ名	1.3.6.1.4.1.18334.1.1.2.1.5.8.5.1.3.1.1
AppleTalk プリンタ名設定		1.3.6.1.4.1.18334.1.1.2.1.5.9.2.1.3.1.1
NetBIOS 設定		1.3.6.1.4.1.18334.1.1.2.1.5.10.1.1.4.1

2.12 HDD 送信ファイルへのアクセス

本機は、管理者設定によって本機管理者が認証されると、HDD 送信ファイルの管理を許可します。

HDD 送信機能とは、スキャンした画像ファイルをユーザー情報とともに本機の HDD に保存する機能です。画像ファイルは「共有」または「個人」として保存できます。本機管理者は PC からのアクセスにより、保存された画像ファイルの一覧表示およびバックアップ（ダウンロード）ができます。

重要
「個人」に保存された画像ファイルが保護対象となります。本機管理者はユーザーに対して機密性の高いファイルを保存する場合は、「個人」を使用するよう管理を行ってください。

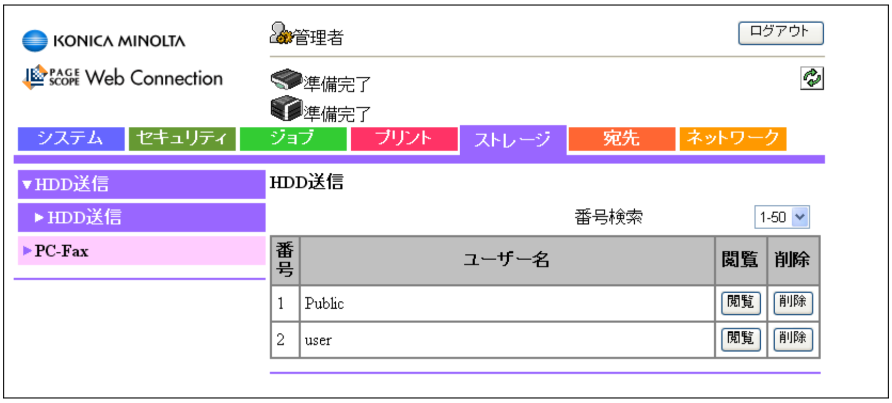
画像ファイルへのアクセスのしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

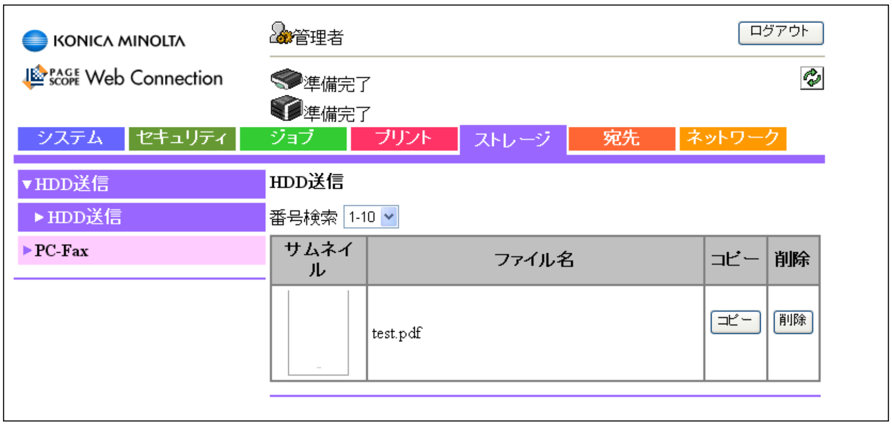
✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ストレージ］タブをクリックし、目的のファイルが保存されているユーザー名の［閲覧］をクリックします。

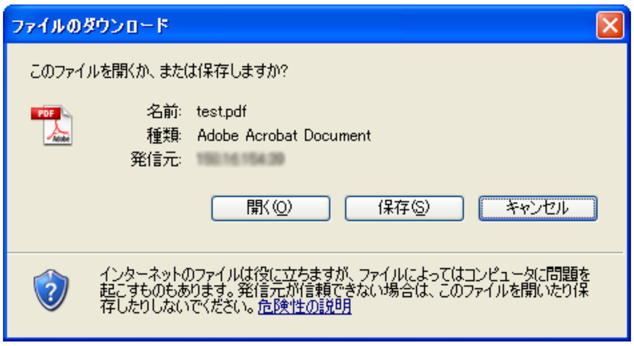


3 保存されている画像ファイルの一覧が表示されます。
バックアップ（ダウンロード）する場合は、目的のファイルの［コピー］をクリックします。



→ ［削除］を選択すると、確認メッセージが表示されます。［OK］をクリックすると指定したファイルは削除されます。

4 ［保存］を選択すると、PC に画像ファイルをバックアップ（ダウンロード）できます。



➔ バックアップ（ダウンロード）しても、本機からファイルは削除されません。

2.13　TCP/IP 設定機能

本機は、管理者設定によって本機管理者が認証されると、IP アドレスの設定および DNS サーバーの登録を行うことができます。

2.13.1　IP アドレスの設定のしかた

＜操作パネルからの設定＞

✔ 管理者設定の表示のしかたは、2-2 ページをごらんください。

✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

1 操作パネルより管理者設定画面を表示させます。

2 ［↓］を押します。

3 ［イーサネット］を押します。

4 ［TCP/IP］を押します。

5 ［IP アドレス］を押します。

6 ［アドレス］を押し、IP アドレスの設定を行います。

7 ［OK］を押します。

8 ［OK］を押し、［閉じる］を押します。

＜ PageScope Web Connection からの設定＞

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ネットワーク］タブをクリックし、［TCP/IP 設定］の［IPv4 設定］をクリックします。

3 Auto IP のチェックボックスを外します。

4 IP アドレスボックスに IP アドレスを入力します。

　➔ 手順 3 の IP 確定方法で Auto IP を選択した場合、DHCP 設定、BootP 設定、ARP/PING 設定、Auto IP 設定など IP アドレスを自動で取得するための手段を選択し、チェックボックスをクリックします。

5 ［適用］をクリックします。

2.13.2　DNS サーバーの登録のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ネットワーク］タブをクリックし、［TCP/IP 設定］の［DNS 設定］をクリックします。

3 DNS サーバーのボックスにアドレスを入力します。

4 各種設定を行います。

5 ［適用］をクリックします。

2.14 NetWare 設定機能

本機は、管理者設定によって本機管理者が認証されると、プリントサーバーとしての登録を行うことができます。

NetWare 設定の設定のしかた

＜操作パネルからの設定＞

✔ イーサネット画面の表示のしかたは、2-35 ページの手順 1 ～ 3 をごらんください。

✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

1 操作パネルよりイーサネット画面を表示させます。

2 ［Netware］を押します。

3 ［使用する］を押し、［OK］を押します。

4 ［閉じる］を押します。

＜ PageScope Web Connection からの設定＞

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ネットワーク］タブをクリックし、［NetWare 設定］をクリックします。

3 各種設定を行います。

4 ［適用］をクリックします。

2.15 SMB 設定機能

本機は、管理者設定によって本機管理者が認証されると、SMB 設定を行うことができます。

SMB 設定の設定のしかた

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。
✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ネットワーク］タブをクリックし、［SMB 設定］をクリックします。

3 各種設定を行います。

4 ［適用］をクリックします。

2.16 AppleTalk 設定機能

本機は、管理者設定によって本機管理者が認証されると、AppleTalk 設定を行うことができます。

AppleTalk 設定の設定のしかた

＜操作パネルからの設定＞

✔ イーサネット画面の表示のしかたは、2-35 ページの手順 1 ～ 3 をごらんください。

✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

1 操作パネルよりイーサネット画面を表示させます。

2 ［AppleTalk］を押します。

3 ［有効］を押し、［OK］を押します。

4 ［閉じる］を押します。

＜ PageScope Web Connection からの設定＞

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。

✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ネットワーク］タブをクリックし、［AppleTalk 設定］をクリックします。

3 各種設定を行います。

4 ［適用］をクリックします。

2.17 E-mail 設定機能

本機は、管理者設定によって本機管理者が認証されると、SMTP サーバー（メールサーバー）の設定を行うことができます。

SMTP サーバー（メールサーバー）の設定のしかた

＜操作パネルからの設定＞

✔ TCP/IP 画面の表示のしかたは、2-35 ページの手順 1 ～ 4 をごらんください。
✔ 管理者設定の設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者設定をログアウトしてください。

1 操作パネルより TCP/IP 画面を表示させます。

2 ［↓］を押します。

3 ［SMTP］を押します。

4 ［有効］を押し、［OK］を押します。

5 ［閉じる］を押します。

＜ PageScope Web Connection からの設定＞

✔ 管理者モードへのアクセスのしかたは、2-2 ページをごらんください。
✔ 管理者モードの設定画面を表示させたままその場を離れないでください。やむを得ずその場を離れる場合は、必ず管理者モードをログアウトしてください。

1 PageScope Web Connection を起動し、管理者モードにアクセスします。

2 ［ネットワーク］タブをクリックし、［E-mai 設定］の［E-mail 送信（SMTP)］をクリックします。

3 各種設定を行います。

4 ［適用］をクリックします。

3 ユーザー編

3 ユーザー編

3.1 ユーザー認証機能

本機能は、管理者設定の認証方式にて［デバイス］または［外部サーバー］（Active Directory）が設定されている場合、本機を使用する前にユーザーが正当な利用者であることを 8 桁以上 64 桁までのユーザーパスワードを使用して認証します。認証中、入力されたパスワードは、「＊」または「●」として表示されます。パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。

また、各アプリケーションソフトからのユーザー認証操作において、保護対象資産に対して影響をおよぼすことのない場合でも、パスワードの誤入力は不正アクセスとしてカウントします。操作方法について、詳しくは各ユーザーズガイドをごんらください。

重要
本機の運用にあたり、本機管理者によって登録されたユーザーパスワードは、ユーザー自身によってユーザーパスワードの変更を行ったのちご使用ください。ユーザーパスワードの変更のしかたについて詳しくは 3-16 ページをごらんください。ユーザー名およびユーザーパスワードについて詳しくは本機管理者におたずねください。

本機運用中、本機管理者によってユーザーパスワードが変更された場合、速やかにユーザー自身が、ユーザーパスワードの変更を行ってください。

ユーザーパスワードは絶対に他のユーザーには知られないようにしてください。

本機管理者により IC カード機能が設定されていると、ユーザー名とユーザーパスワードを入力する認証のほかに、IC カードを使用した認証ができます。

認証方式	内容
なし	ユーザー認証に IC カードを使用しません。ユーザー名とユーザーパスワードを入力して認証する方式です。
カード認証	ユーザー名とユーザーパスワードを入力する認証のほかに、IC カードを使用して識別する方式です。
カード認証 + パスワード	ユーザー名とユーザーパスワードを入力する認証のほかに、IC カードを IC カードリーダーに置いたあと、ユーザーパスワードを入力して認証する方式です。

参考
- IC カードで認証する場合は､あらかじめ本機管理者が IC カード機能を設定し､IC カードに記録された情報を本機に登録する必要があります。詳しくは本機管理者にご確認ください。
- IC カードによる認証は［デバイス］設定時のみ利用可能です。
- PageScope Web Connection やプリンタードライバーからの印刷など、本機以外から認証を行う場合は、IC カードによる認証はできません。

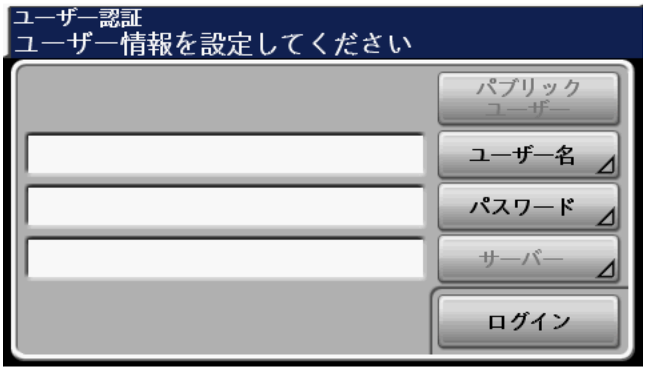
3.1.1　ユーザー認証のしかた（ユーザー名 / ユーザーパスワード入力による認証）

<操作パネルからのアクセス>

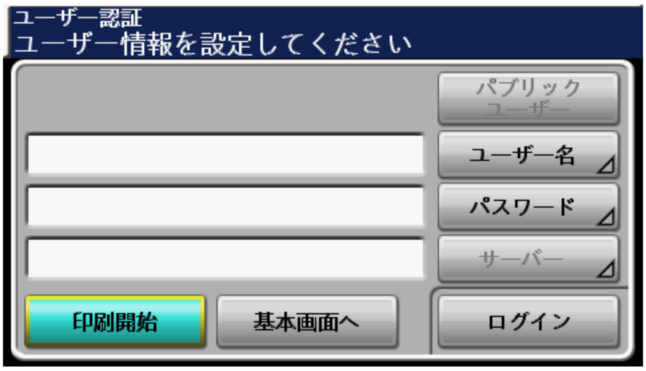
✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

✔ 認証方式にて［外部サーバー］（Active Directory）が設定されている場合、ユーザー認証にて認証されると、本機に登録されていないユーザー名は自動的に登録されます。

1　［ユーザー名］を押します。



➔ 認証＆プリント機能が設定されている場合は、下記の画面が表示されます。
ただし認証＆プリント機能が設定されていないと、認証＆プリントファイルが本機に保存されていても、［印刷開始］または［基本画面へ］は表示されません。通常にログインした後、［認証＆プリント］から目的のファイルを選択し、印刷してください。認証＆プリントファイルへのアクセスのしかたについて詳しくは 3-14 ページをごらんください。



2　［直接入力］を押します。



3　キーボードまたはテンキーでユーザー名を入力します。



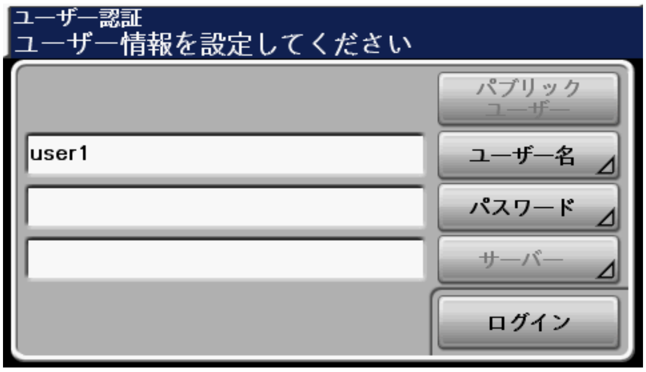
➔ ［C］を押すと、入力された値がクリアされます。
➔ ［削除］を押すと、入力した文字が 1 文字ずつ削除されます。
➔ ［↑］を押すと、大文字画面に切り替わります。
➔ ［!#?/］を押すと、記号画面に切り替わります。

4　［OK］を押します。

5　［OK］を押します。



6　［パスワード］を押します。



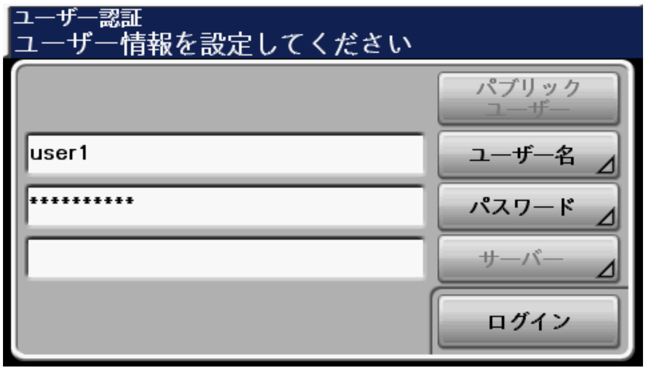
7 キーボードまたはテンキーで 8 桁以上 64 桁までのユーザーパスワードを入力します。



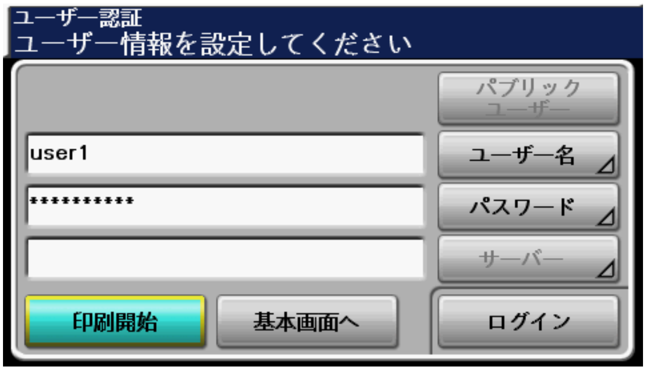
➔ ［C］を押すと、入力された値がクリアされます。
➔ ［削除］を押すと、入力した文字が 1 文字ずつ削除されます。
➔ ［↑］を押すと、大文字画面に切り替わります。
➔ ［!#?/］を押すと、記号画面に切り替わります。

8 ［OK］を押します。

9 ［ログイン］を押します。



➔ 認証＆プリントファイルが保存されている場合は、［印刷開始］または［基本画面へ］を選択してから［ログイン］を押します。



ログイン方法	説明
［印刷開始］	該当ユーザーの認証＆プリントファイルの印刷のみを行います。ユーザーモード画面には移行しません。
［基本画面へ］	通常のログインのみとなり、認証＆プリントファイルは出力されません。

➔ ユーザー名を間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しいユーザー名を入力してください。

➔ ユーザーパスワードを間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。

➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

➔ 複数の認証＆プリントファイルがある場合は、すべての認証＆プリントファイルが印刷されます。目的のファイルを選択して印刷したい場合は、［基本画面へ］を選択し、［認証＆プリント］から目的のファイルを選択し、印刷してください。認証＆プリントファイルへのアクセスのしかたについて詳しくは 3-14 ページをごらんください。

➔ 認証＆プリント機能が設定されていても、認証＆プリントファイルが保存されていない場合は、［印刷開始］または［基本画面へ］のどちらを選択しても通常のログインとなります。

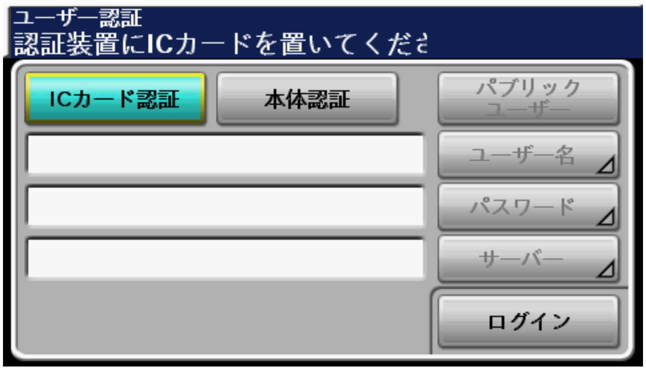
10 ［ID］を押すと、ログアウトします。

3.1.2 ユーザー認証のしかた（IC カードによる識別）

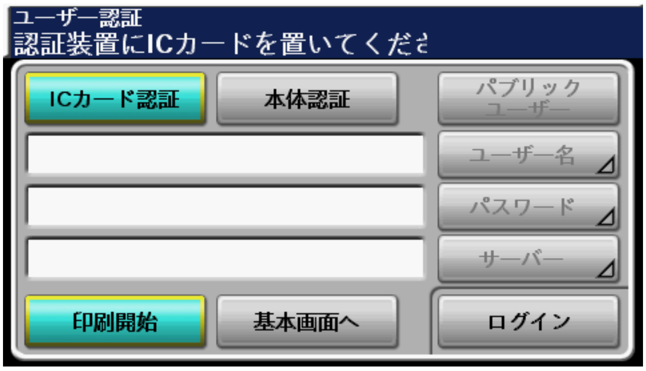
<操作パネルからのアクセス>

✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

1 ［IC カード認証］を押します。



→ 認証＆プリント機能が設定されている場合は、下記の画面が表示されます。
ただし認証＆プリント機能が設定されていないと、認証＆プリントファイルが本機に保存されていても、［印刷開始］または［基本画面へ］は表示されません。通常にログインした後、［認証＆プリント］から目的のファイルを選択し、印刷してください。認証＆プリントファイルへのアクセスのしかたについて詳しくは 3-14 ページをごらんください。



2 IC カードリーダーに IC カードを置くとログインできます。
認証＆プリントファイルが保存されている場合は、［印刷開始］または［基本画面へ］を選択してから IC カードリーダーに IC カードを置きます。

ログイン方法	説明
［印刷開始］	該当ユーザーの認証＆プリントファイルの印刷のみを行います。ユーザーモード画面には移行しません。
［基本画面へ］	通常のログインのみとなり、認証＆プリントファイルは出力されません。

→ 複数の認証＆プリントファイルがある場合は、すべての認証＆プリントファイルが印刷されます。目的のファイルを選択して印刷したい場合は、［基本画面へ］を選択し、［認証＆プリント］から目的のファイルを選択し、印刷してください。認証＆プリントファイルへのアクセスのしかたについて詳しくは 3-14 ページをごらんください。

→ 認証＆プリント機能が設定されていても、認証＆プリントファイルが保存されていない場合は、［印刷開始］または［基本画面へ］のどちらを選択しても通常のログインとなります。

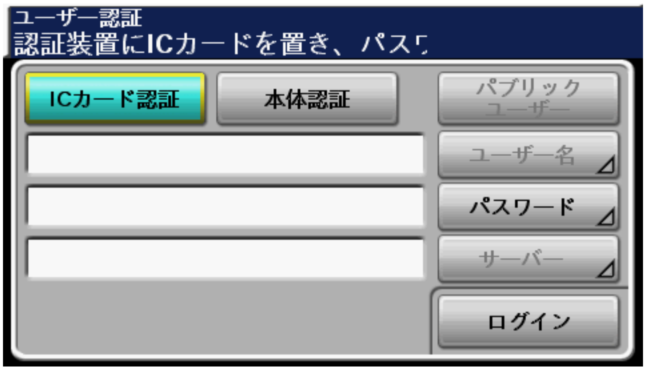
3 ［ID］を押すと、ログアウトします。

3.1.3 ユーザー認証のしかた（IC カード＋ユーザーパスワードによる認証）

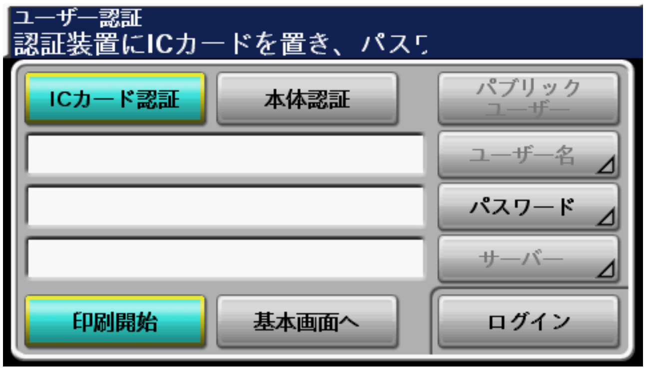
＜操作パネルからのアクセス＞

✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

1 ［IC カード認証］を押します。

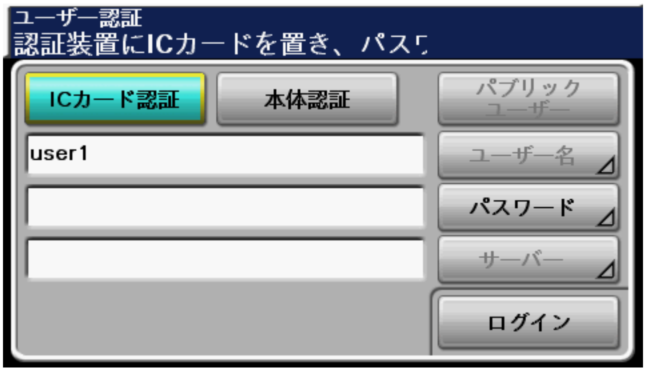


➔ 認証＆プリント機能が設定されている場合は、下記の画面が表示されます。
ただし認証＆プリント機能が設定されていないと、認証＆プリントファイルが本機に保存されていても、［印刷開始］または［基本画面へ］は表示されません。通常にログインした後、［認証＆プリント］から目的のファイルを選択し、印刷してください。認証＆プリントファイルへのアクセスのしかたについて詳しくは 3-14 ページをごらんください。



2 IC カードリーダーに IC カードを置きます。

3 ［パスワード］を押します。



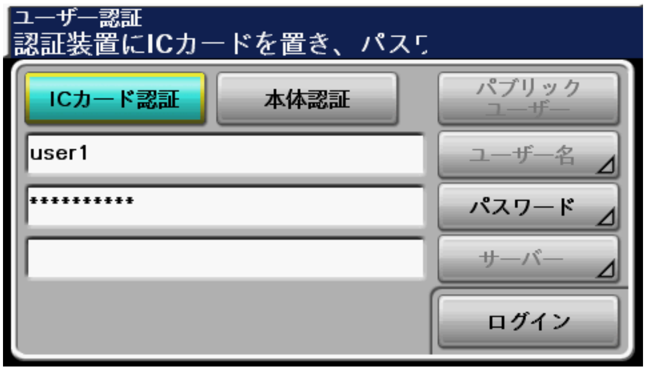
4 キーボードまたはテンキーで 8 桁以上 64 桁までのユーザーパスワードを入力します。



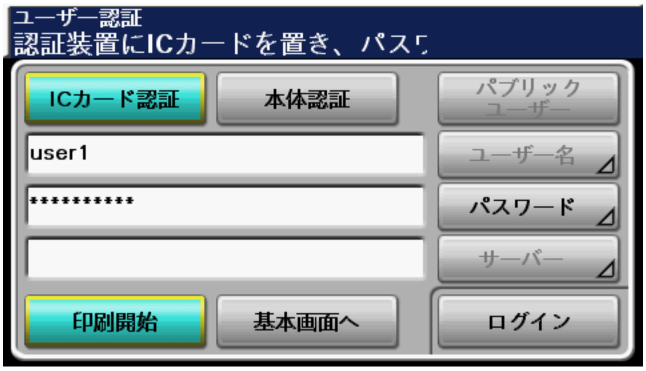
→ ［C］を押すと、入力された値がクリアされます。
→ ［削除］を押すと、入力した文字が 1 文字ずつ削除されます。
→ ［↑］を押すと、大文字画面に切り替わります。
→ ［!#?/］を押すと、記号画面に切り替わります。

5 ［OK］を押します。

6 ［ログイン］を押します。



→ 認証＆プリントファイルが保存されている場合は、［印刷開始］または［基本画面へ］を選択してから［ログイン］を押します。



ログイン方法	説明
［印刷開始］	該当ユーザーの認証＆プリントファイルの印刷のみを行います。ユーザーモード画面には移行しません。
［基本画面へ］	通常のログインのみとなり、認証＆プリントファイルは出力されません。

➔ ユーザーパスワードを間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。

➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

➔ 複数の認証＆プリントファイルがある場合は、すべての認証＆プリントファイルが印刷されます。目的のファイルを選択して印刷したい場合は、［基本画面へ］を選択し、［認証＆プリント］から目的のファイルを選択し、印刷してください。認証＆プリントファイルへのアクセスのしかたについて詳しくは 3-14 ページをごらんください。

➔ 認証＆プリント機能が設定されていても、認証＆プリントファイルが保存されていない場合は、［印刷開始］または［基本画面へ］のどちらを選択しても通常のログインとなります。

7 ［ID］を押すと、ログアウトします。

< PageScope Web Connection からのアクセス>

✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

✔ 認証方式にて［外部サーバー］(Active Directory）が設定されている場合、ユーザー認証にて認証されたユーザー名は、本機内に自動的に登録されます。

1 Web ブラウザを起動させます。

2 アドレスバーに本機の IP アドレスを入力します。

3 ［Enter］キーを押し、PageScope Web Connection を起動します。

4 レジスタユーザーのラジオボタンをクリックし、ユーザー名およびユーザーパスワードを入力します。



5 ［ログイン］をクリックします。

➔ ユーザーパスワードを間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。

➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

6 ログアウトする場合は、［ログアウト］をクリックします。

3.2 認証＆プリント機能

本機は、ユーザー認証にて認証されたすべてのユーザーに、認証＆プリントファイルの登録およびアクセスを許可します。

本機管理者により認証＆プリント機能が設定されていると、操作パネルで認証が成功したあと、本機のHDD に保存された該当ユーザーの印刷データを、自動的に印刷することができます。本機の操作パネルでユーザー認証後に出力するので、機密性の高い文書の出力に便利です。

参考

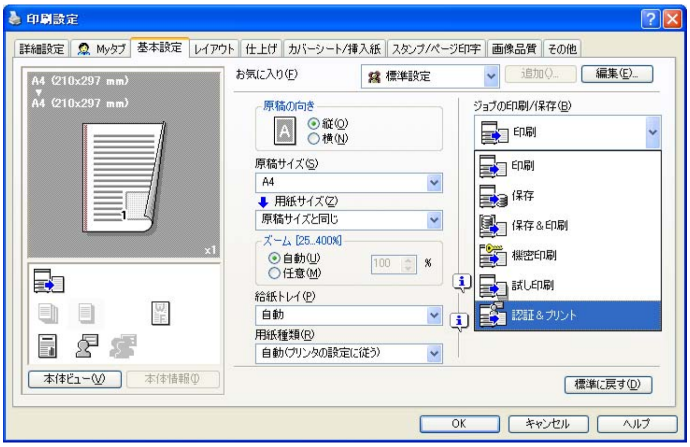
- 本機管理者が認証＆プリント機能を設定している場合は、プリンタードライバー側で［印刷］を選択しても、認証＆プリントファイルとして保存されます。
- 本機管理者が認証＆プリント機能を設定していなくても、プリンタードライバー側で［認証＆プリント］を選択すると、認証＆プリントファイルとして保存されます。
- 本機管理者が認証＆プリント機能を設定している場合は、PageScope Web Connection からのダイレクトプリントファイルも認証＆プリントファイルとして保存されます。

3.2.1 認証＆プリントファイルの登録のしかた

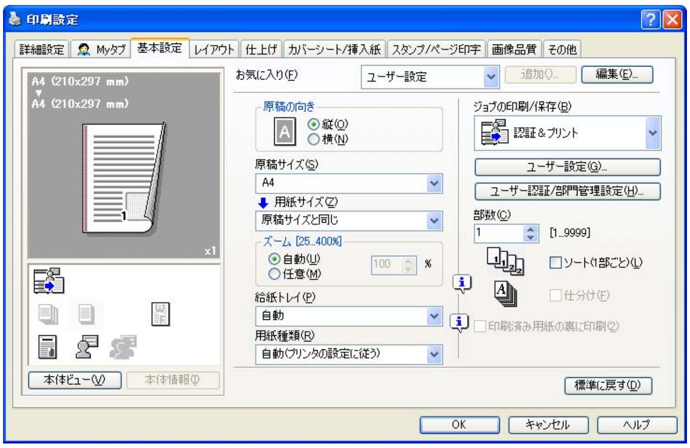
1 印刷ダイアログボックスで［プロパティ］をクリックして、印刷設定画面を表示させます。

2 ［基本設定］タブをクリックします。

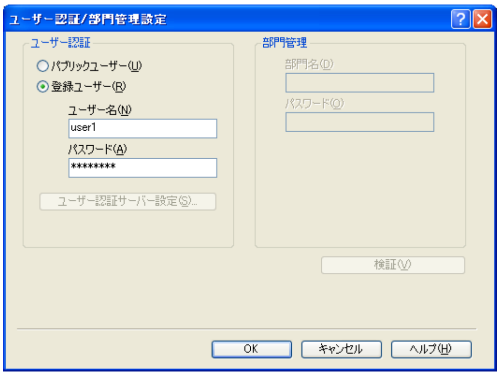
3 ［ジョブの印刷 / 保存］で［認証＆プリント］を選択します。



4 ［ユーザー認証 / 部門管理設定］をクリックします。



5 ユーザー名とユーザーパスワードを入力し、［OK］をクリックします。



➔ 入力したユーザー名に対してユーザーパスワードが一致していない場合、認証＆プリントファイルは本機に登録されず破棄されます。

➔ ユーザー名に「"」（ダブルクォーテーション）を含むユーザーを指定して印刷や保存をおこなうと、本機側でログインエラーとなりプリントジョブは破棄されます。

➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

6 印刷します。

3.2.2　　認証＆プリントファイルへのアクセスのしかた

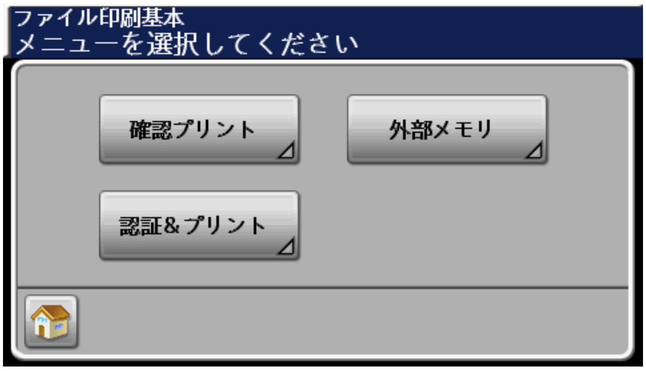
✔ ログインのしかたは、3-2 ページをごらんください。
✔ ユーザーモードにログインしたままその場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

1 操作パネルよりユーザー認証にてユーザーモードにログインします。

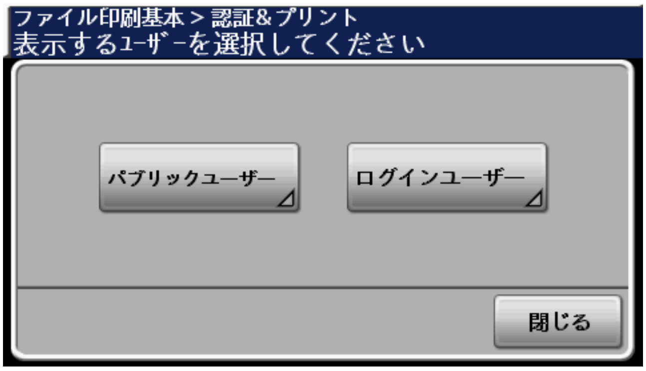
2 ［USB/HDD］を押します。



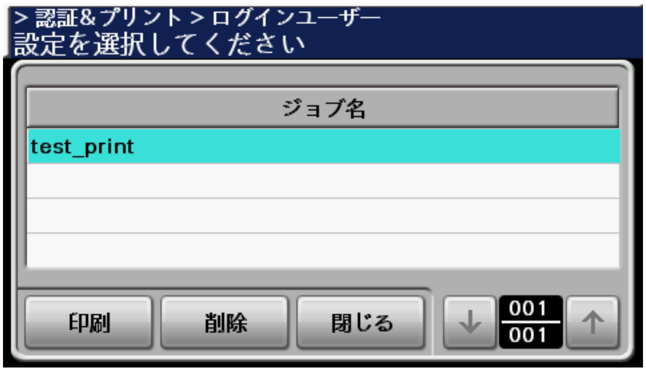
3 ［認証＆プリント］を押します。



4 ［ログインユーザー］を押します。



5 目的の認証＆プリントファイルを選択し、［印刷］を押します。



➔ 認証＆プリントファイルは、印刷が正常に終了した時点で自動的に削除されます。

3.3 パスワード変更機能

本機は、ユーザー認証の認証方式にて［デバイス］が設定されている場合、ユーザー認証にて認証されたすべてのユーザーに、ユーザー自身のユーザーパスワードの変更操作を許可します。

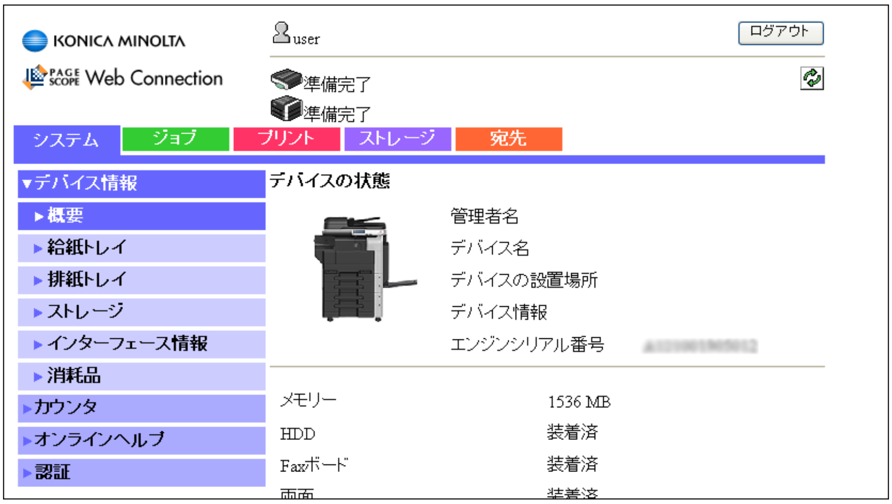
入力されたパスワードは、「●」として表示されます。

パスワード変更のしかた

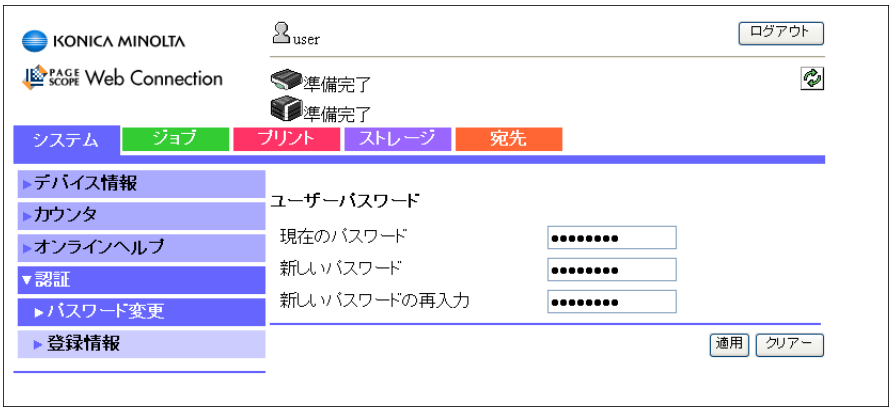
✔ ログインのしかたは、3-2 ページをごらんください。
✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。
✔ ユーザーパスワードは定期的に変更してください。
✔ ユーザーパスワードは絶対に他のユーザーには知られないようにしてください。
✔ ユーザーパスワードには誕生日、社員番号等から推測可能な番号を設定しないでください。

1 PageScope Web Connection よりユーザー認証にてユーザーモードにログインします。

2 ［システム］タブの［認証］をクリックします。



3 現在登録されているユーザーパスワードおよび新しいユーザーパスワードを入力し、誤入力防止のため再度新しいユーザーパスワードを入力します。



4 ［適用］をクリックします。

➔「現在のパスワード」ボックスにユーザーパスワードを間違えて入力した場合、ユーザーパスワードが一致していないことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。

➔「新しいパスワード」ボックスに入力したユーザーパスワードがパスワード規約の条件を満たしていない場合、入力したユーザーパスワードは使用できないことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。パスワード規約について詳しくは、1-8 ページをごらんください。

➔「新しいパスワード」と「新しいパスワードの再入力」ボックスに入力したユーザーパスワードが一致していない場合、ユーザーパスワードが一致していないことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。

3.4　機密印刷機能

本機能は、PC 側よりパスワード指定された機密印刷ファイルが本機に登録された状態で利用される機能です。

機密印刷ファイルにアクセスする場合、機密印刷ファイルの正当な利用者であることを 8 桁のパスワードを使用して認証します。入力されたパスワードは、「＊」として表示されます。パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。

3.4.1　機密印刷ファイルの登録のしかた

✔ 機密印刷パスワードには、パスワード規約の条件を満たした 8 桁のパスワードを入力してください。パスワード規約について詳しくは、1-8 ページをごらんください。

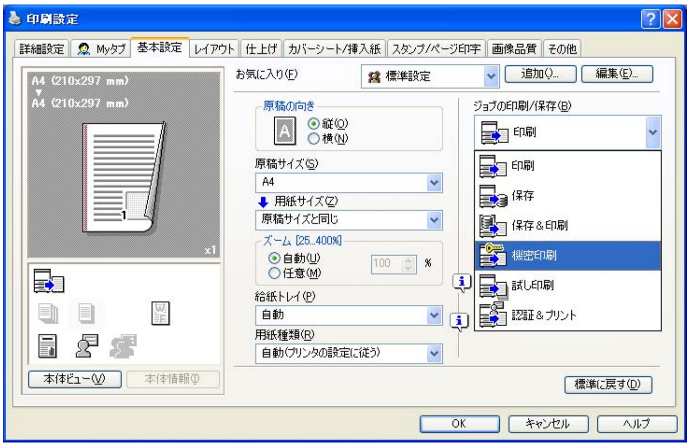
✔ 機密印刷パスワードは絶対に他のユーザーには知られないようにしてください。

✔ 機密印刷パスワードには誕生日、社員番号等から推測可能な番号を設定しないでください。

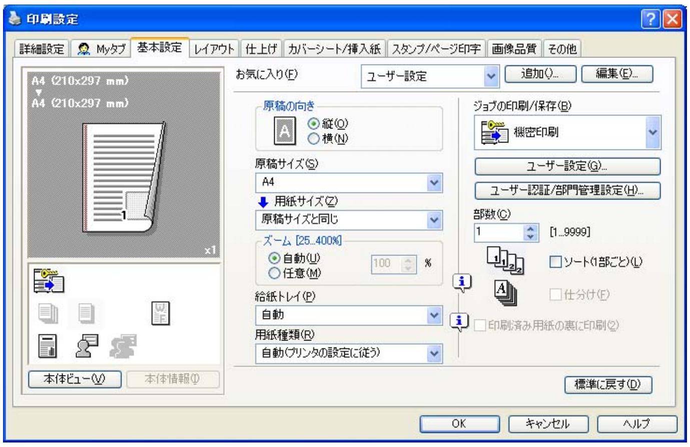
1 印刷ダイアログボックスで［プロパティ］をクリックして、印刷設定画面を表示させます。

2 ［基本設定］タブをクリックします。

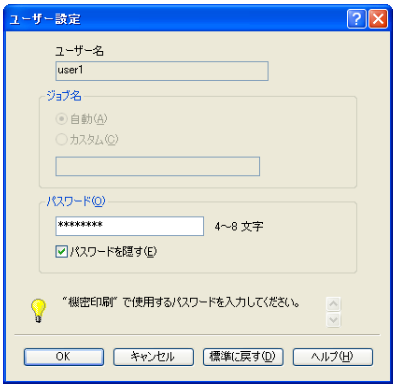
3 ［ジョブの印刷 / 保存］で［機密印刷］を選択します。



4 ［ユーザー設定］をクリックします。



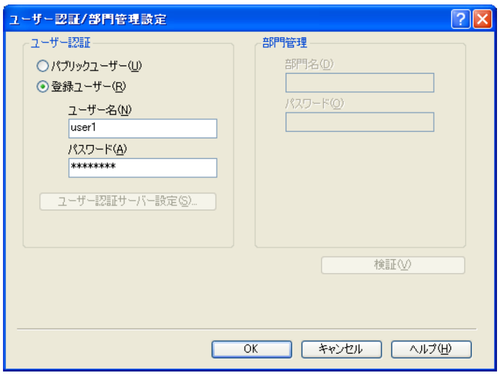
5　パスワードボックスに 8 桁の機密印刷パスワードを入力します。



6　［OK］をクリックします。

7　［ユーザー認証 / 部門管理設定］をクリックします。

8　ユーザー名とユーザーパスワードを入力し、［OK］をクリックします。



- ➔ 入力されたユーザー名に対してユーザーパスワードが一致していない場合、機密印刷ファイルは本機に登録されず破棄されます。
- ➔ ユーザー名に「"」（ダブルクォーテーション）を含むユーザーを指定して印刷や保存をおこなうと、本機側でログインエラーとなりプリントジョブは破棄されます。
- ➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

9　印刷します。

3.4.2　　機密印刷ファイルへのアクセス

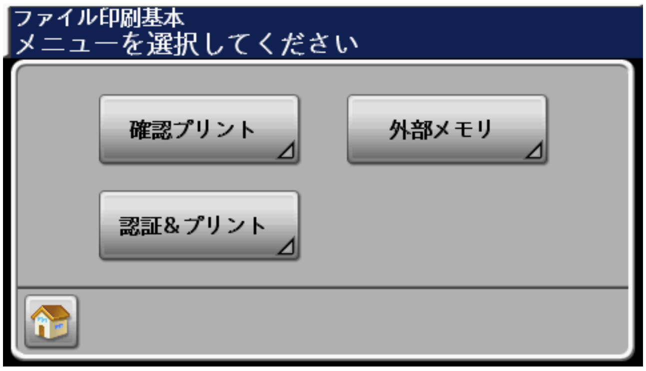
✔　ログインのしかたは、3-2 ページをごらんください。
✔　ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。
✔　機密印刷パスワードは、PC 側のプリンタードライバーにて行ってください。入力されたパスワードは「＊」として表示されます。

1　操作パネルよりユーザー認証にてユーザーモードにログインします。

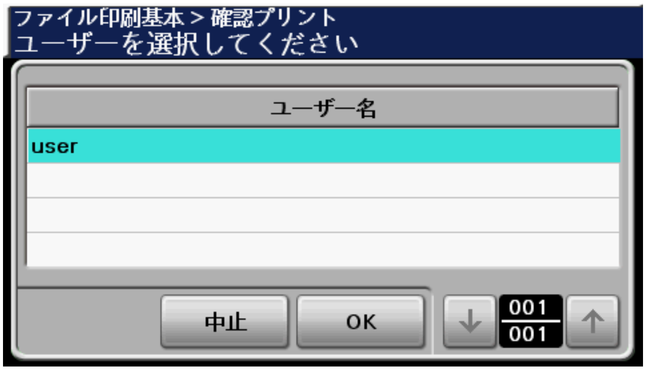
2　［USB/HDD］を押します。



3　［確認プリント］を押します。

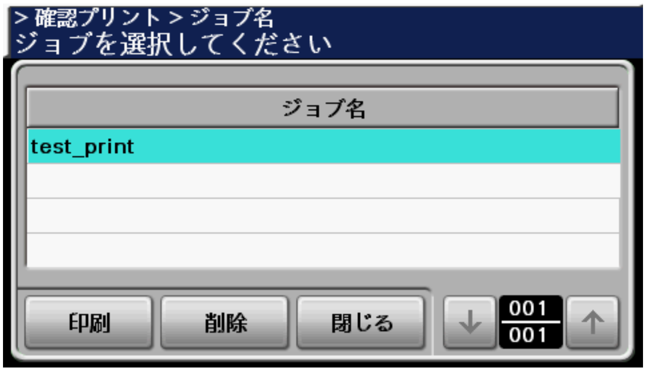


4　ユーザーを選択し、［OK］を押します。

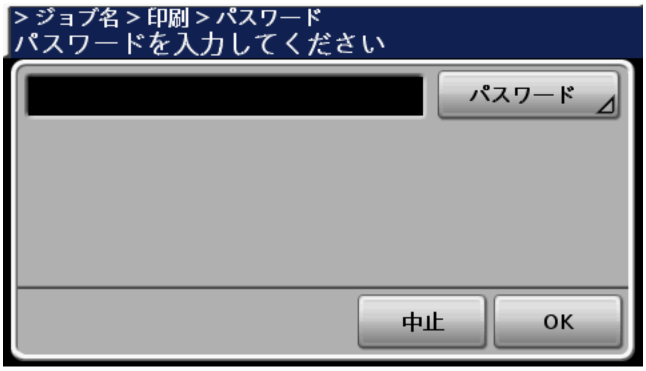


➔　機密印刷ファイル を送信した PC のユーザー名が表示されます。

5 目的の機密印刷ファイルを選択し、[印刷] を押します。



6 [パスワード] を押します。



7 キーボードまたはテンキーで 8 桁の機密印刷パスワードを入力します。



- ➔ 機密印刷パスワードには、プリンタードライバー側で設定した 8 桁の機密印刷パスワードを入力してください。
- ➔ [C] を押すと、入力された値がクリアされます。
- ➔ [削除] を押すと、入力した文字が 1 文字ずつ削除されます。
- ➔ [↑] を押すと、大文字画面に切り替わります。
- ➔ [!#?/] を押すと、記号画面に切り替わります。

8 [OK] を押します。

9 ［OK］を押します。



➔ 機密印刷パスワードを間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しい機密印刷パスワードを入力してください。
➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

10 内容を確認し、［OK］を押します。



➔ ［中止］を押すと、手順 5 の画面に戻ります。
➔ 機密印刷ファイルは、印刷が正常に終了した時点で自動的に削除されます。

3.5 HDD 送信機能

本機は、ユーザー認証にて認証されたすべてのユーザーに HDD 送信機能の操作を許可します。また、HDD に保存された画像ファイルの取得やプリント操作を許可します。

HDD 送信機能とは、スキャンした画像ファイルをユーザー情報とともに本機の HDD に保存する機能です。画像ファイルは「共有」または「個人」として保存できます。保存された画像ファイルは、操作パネルまたは PC からのユーザー名とパスワードの認証によりアクセスすることができます。

本機から画像ファイルを PC にダウンロードする際には、SSL/TLS プロトコルを使用した暗号化通信が行われるため、データは保護されます。

3.5.1 画像ファイルの登録のしかた

✔ ログインのしかたは、3-2 ページをごらんください。

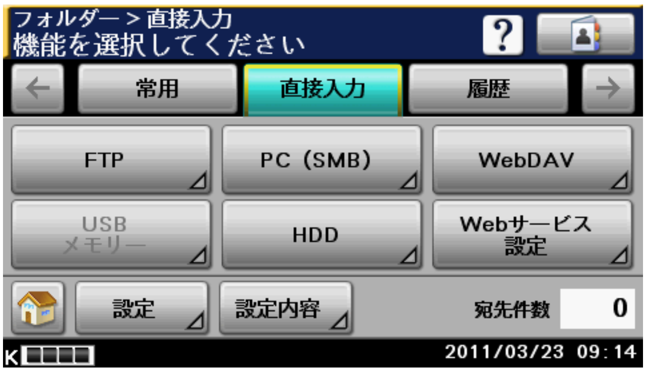
✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

1 操作パネルよりユーザー認証にてユーザーモードにログインします。

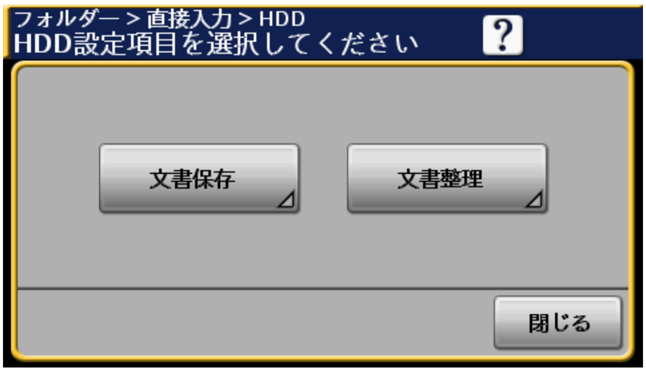
2 ［ファイル送信］を押します。



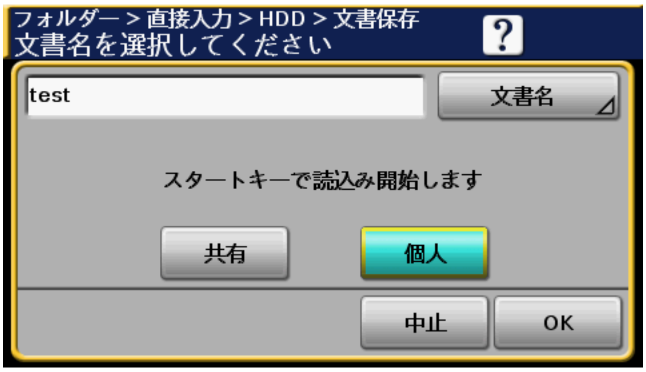
3 ［直接入力］タブを押し、［HDD］を押します。



4 ［文書保存］を押します。



5　保存先を選択し、［OK］または［スタート］を押します。



➔［個人］に保存された画像ファイルが保護対象となります。機密性の高いファイルを保存する場合は、［個人］を選択してください。

3.5.2 画像ファイルへのアクセスのしかた

＜操作パネルからのアクセス＞

✔ ログインのしかたは、3-2 ページをごらんください。

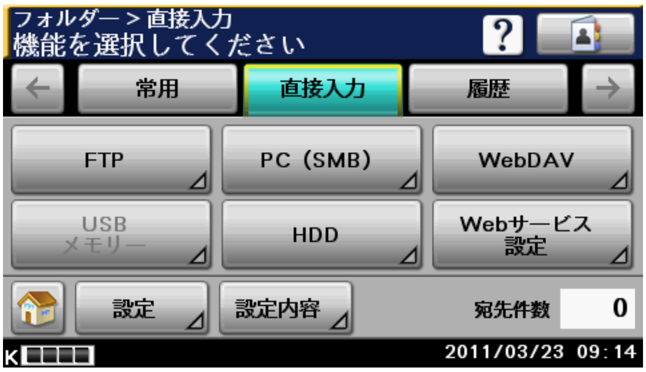
✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

1 操作パネルよりユーザー認証にてユーザーモードにログインします。

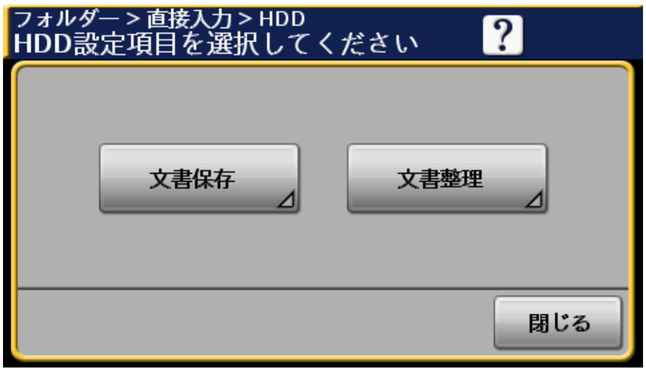
2 ［ファイル送信］を押します。



3 ［直接入力］タブを押し、［HDD］を押します。



4 ［文書整理］を押します。



5 保存されている文書の一覧が表示されます。



➔ ファイルを削除する場合は、削除したい文書を選択し、[削除]を押します。

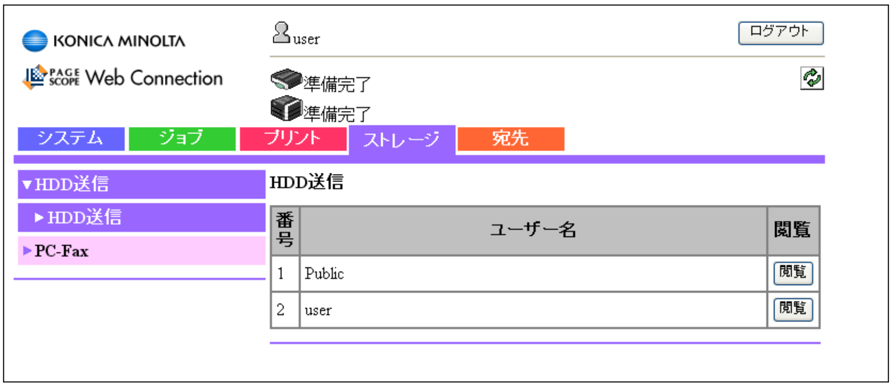
< PageScope Web Connection からのアクセス>

✔ ログインのしかたは、3-2 ページをごらんください。

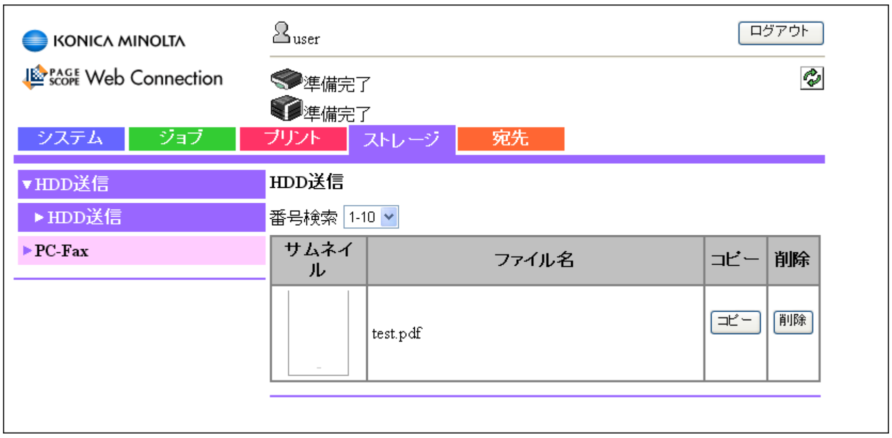
✔ ユーザーモードにログイン中その場を離れないでください。やむを得ずその場を離れる場合は、必ずユーザーモードをログアウトしてください。

1 PageScope Web Connection よりユーザー認証にてユーザーモードにログインします。

2 ［ストレージ］タブをクリックし、目的のファイルが保存されているユーザー名の［閲覧］をクリックします。

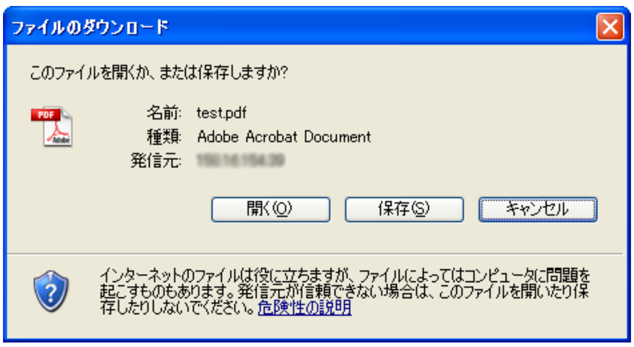


3 目的のファイルの［コピー］をクリックします。



➔ ［削除］を選択すると、確認メッセージが表示されます。［OK］をクリックすると指定したファイルは削除されます。

4 ［開く］または［保存］を選択し、目的の機能を実行してください。



➔ ダウンロードしても、本機からファイルは削除されません。

4 アプリケーションソフト編

4 アプリケーションソフト編

4.1 PageScope Data Administrator について

PageScope Data Administrator とは、本機の認証機能、宛先機能をネットワーク上の PC から編集 / 登録する、管理用のアプリケーションのことをいいます。

本機から、認証リスト、宛先リストをご使用の PC に取り込み、編集したのち、再び本機に書き込むことができます。

XML, CSV, TAB, LDIF, Lotus Notes Structured Text 等のファイル形式の宛先リストを取り込むことができます。また、Active Directory 等のディレクトリサーバーに対して、LDAP プロトコルを使って宛先の検索やブラウズを行い、宛先リストを取り込むことができます。

重要
管理者パスワードは絶対に一般ユーザーには知られないようにしてください。

管理者パスワードを忘れた場合、サービスエンジニアによる設定が必要です。サービス実施店にご連絡ください。

バックアップ、リストア時のご注意

本機は、PageScope Data Administrator を利用して、認証情報や宛先リストなどのデータを、ご使用の PC にバックアップ（取得）し、再度本機にリストア（書込み）できます。バックアップ、リストアを行う場合は、以下の点に注意してください。

- PageScope Data Administrator にて、バックアップやリストアを行う場合、セキュリティ強化設定 OFF 時に取得したバックアップデータを、セキュリティ強化設定有効時には使用しないでください。
- PageScope Data Administrator 以外では、バックアップデータの編集を行わないでください。

4.1.1 PageScope Data Administrator からのアクセスのしかた

✔ PageScope Data Administrator にて本機にアクセス中その場を離れないでください。やむを得ずその場を離れる場合は、必ず PageScope Data Administrator を終了してください。

1 PageScope Data Administrator を起動します。

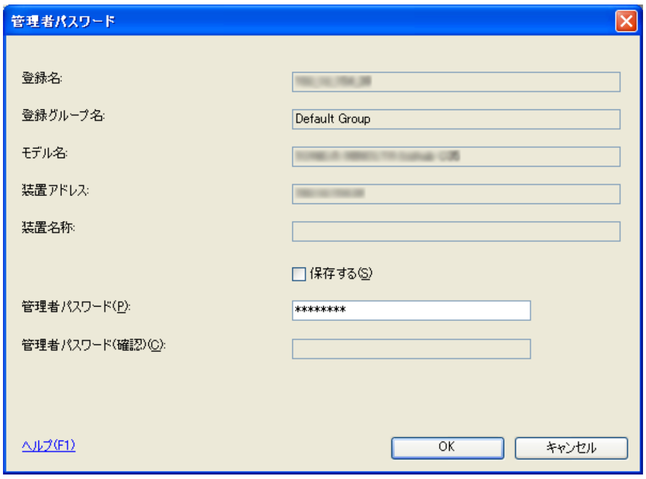
2 装置一覧画面から本機を選択し、［認証設定 / 宛先設定］をクリックします。



3 装置情報の読込み画面の設定を確認し、[読込み]をクリックします。



4 本機に登録されている 8 桁の管理者パスワードを入力し、[OK]をクリックします。



→ 「保存する」のチェックボックスにチェックが入っている場合、入力された管理者パスワードはご使用の PC に記憶されます。管理者パスワードを記憶させたくない方は、「保存する」のチェックボックスのチェックを外してご使用ください。

→ 管理者パスワードを間違えて入力した場合、パスワードが一致していないことを告げるメッセージが表示されます。正しい管理者パスワードを入力してください。

→ 「保存する」のチェックボックスにチェックをした場合、管理者パスワードの確認のため再度 8 桁の管理者パスワードを入力してください。

→ 確認のための管理者パスワードを間違えて入力した場合、パスワードが一致していないことを告げるメッセージが表示されます。正しい管理者パスワードを入力してください。

→ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

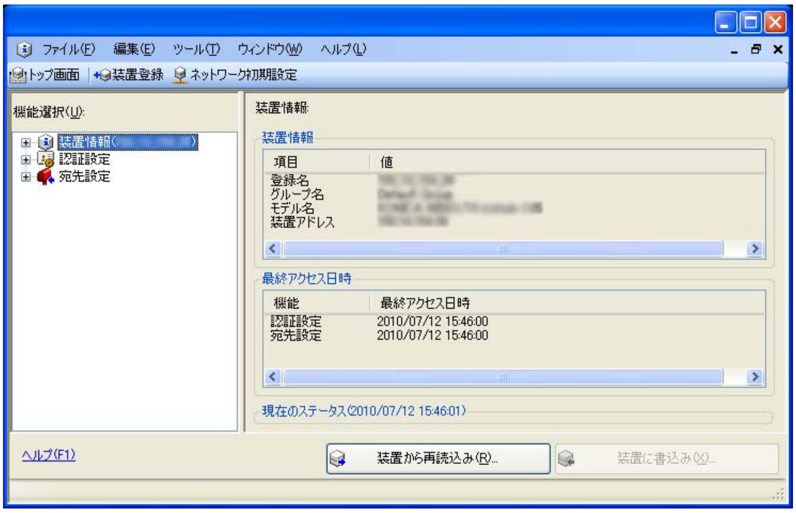
5 SSL 証明書の確認画面の表示内容を確認し、[はい]をクリックします。

4.1.2 ユーザー認証方式の設定のしかた

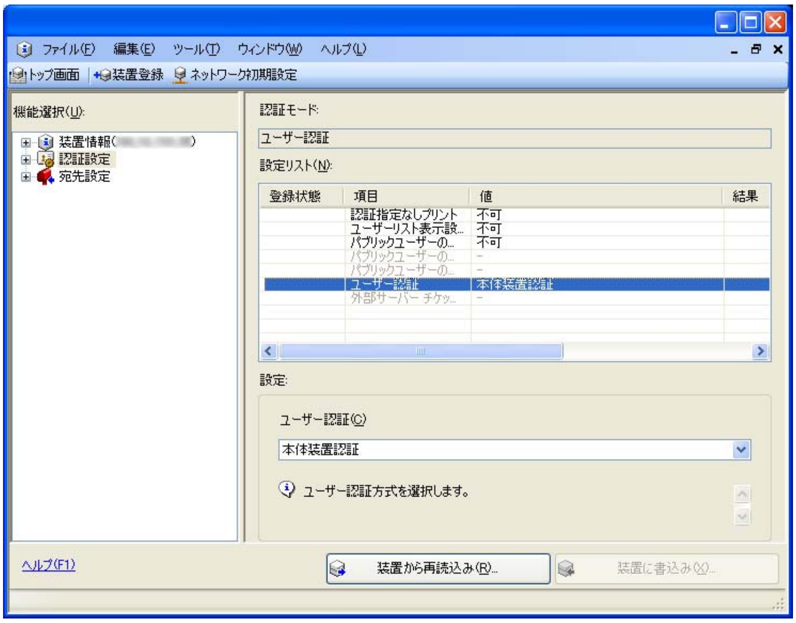
✔ IC カード機能が設定されている場合は、ユーザー認証方式の変更はできません。
✔ 本機へのアクセスのしかたは、4-2 ページの手順 1 ～ 5 をごらんください。
✔ PageScope Data Administrator にて本機にアクセス中その場を離れないでください。やむを得ずその場を離れる場合は、必ず PageScope Data Administrator を終了してください。

1 PageScope Data Administrator の［認証設定 / 宛先設定］モードにて本機にアクセスします。

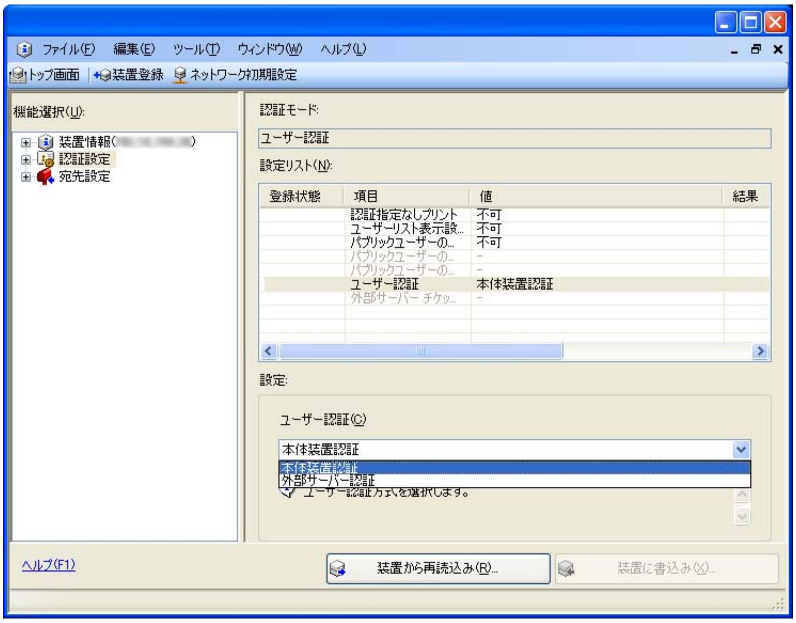
2 ［認証設定］をクリックします。



3 ［ユーザー認証］をクリックします。



4　ユーザー認証のプルダウンメニューからユーザー認証方式を選択します。



➔「本体装置認証」から「外部サーバー認証」に変更する場合、あらかじめ本体側で Active Directory のドメイン名を登録しておいてください。

➔「外部サーバー認証」を選択した場合、必ず「Active Directory」を選択してください。

5　［装置に書込み］をクリックします。

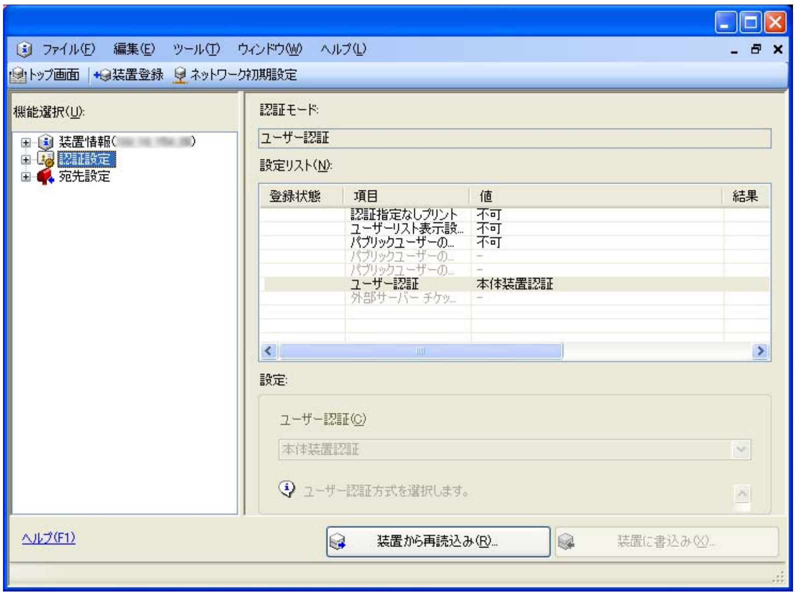
➔ 本機で実行中のジョブまたはジョブ予約（タイマー送信、Fax リダイヤル待ちなど）がされている場合、装置ロックエラーにより書き込みに失敗したことを告げるメッセージが表示されます。［OK］をクリックし、しばらくしてから再度装置への書込みを行ってください。

4.1.3 認証モードの変更のしかた

✔ 本機へのアクセスのしかたは、4-2 ページの手順 1 ～ 5 をごらんください。
✔ PageScope Data Administrator にて本機にアクセス中その場を離れないでください。やむを得ずその場を離れる場合は、必ず PageScope Data Administrator を終了してください。

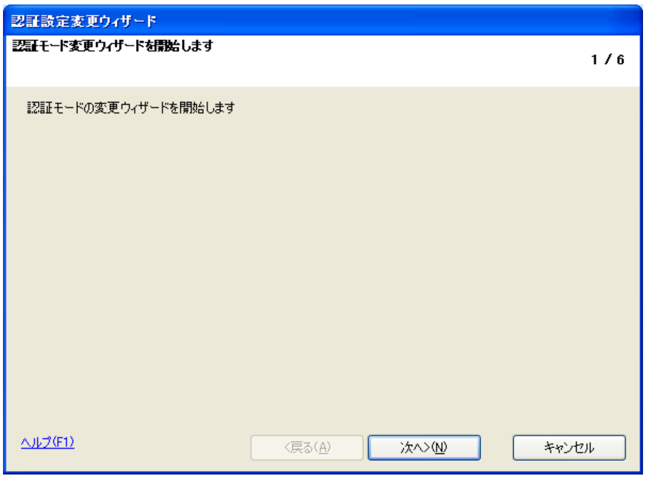
1 PageScope Data Administrator の［認証設定 / 宛先設定］モードにて本機にアクセスします。

2 ［認証設定］をクリックします。

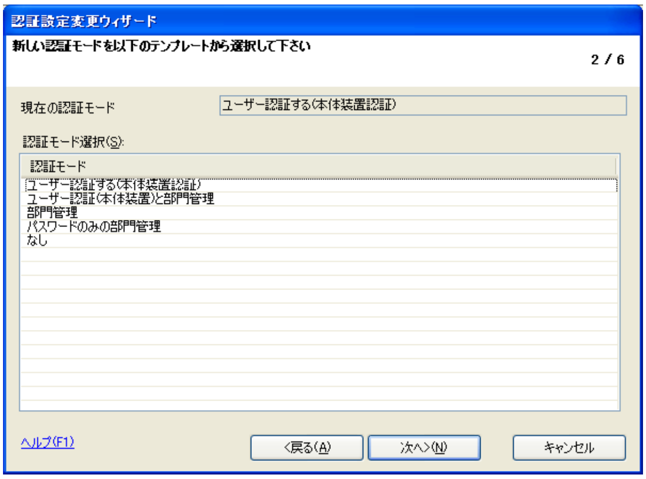


3 ツールバーの［編集］から［認証設定］を選択し、［認証モード変更］をクリックします。

4 ［次へ］をクリックします。



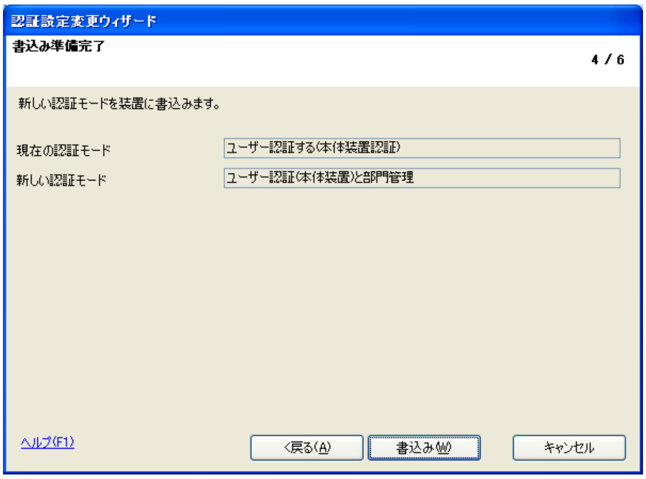
5　変更したい［認証モード］を選択して、［次へ］をクリックします。



→［ユーザー認証と部門管理］を選択した場合は、ユーザー数・部門数の割当を設定してください。

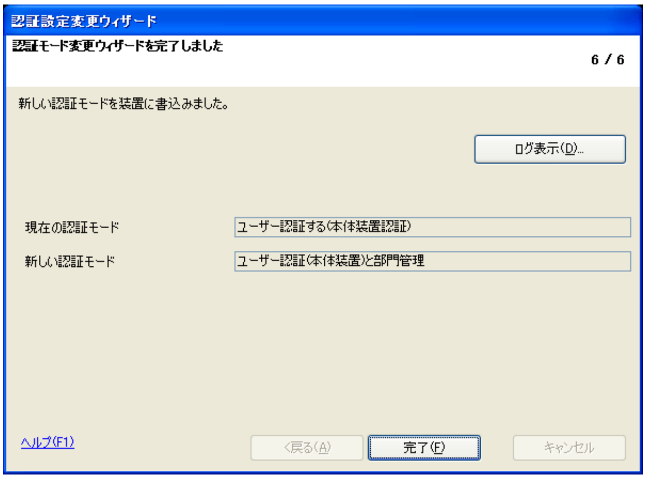


6　新しい認証モードを確認して、［書込み］をクリックします。

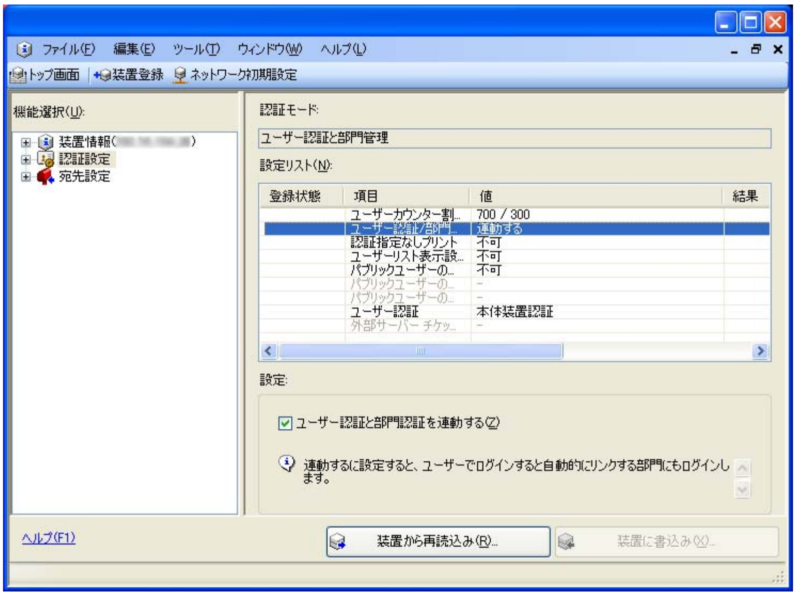


→ 本機で実行中のジョブまたはジョブ予約（タイマー送信、Fax リダイヤル待ちなど）がされている場合、装置ロックエラーにより書き込みに失敗したことを告げるメッセージが表示されます。［OK］をクリックし、しばらくしてから再度装置への書込みを行ってください。

7 ［完了］をクリックします。



➔ 手順 5 で［ユーザー認証と部門管理］を選択した場合は、ユーザー認証 / 部門管理は［連動する］に設定されます。連動させたくない場合は［ユーザー認証と部門管理を連動する］のチェックを外して、再度［装置に書込み］を実行してください。



4.1.4 ユーザー設定のしかた

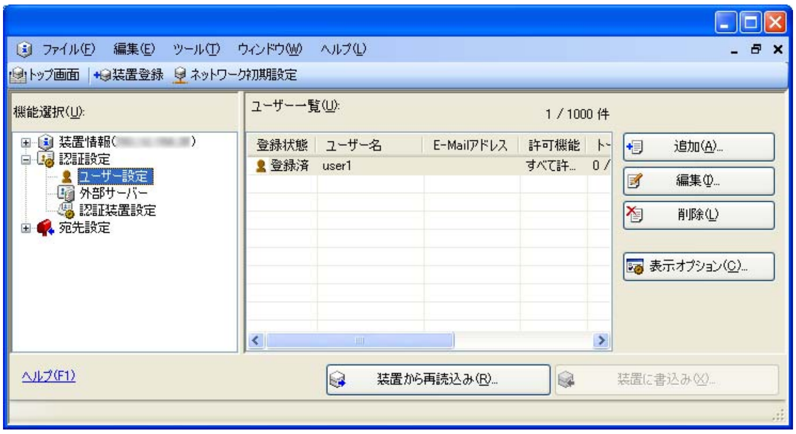
✔ 本機へのアクセスのしかたは、4-2 ページの手順 1 〜 5 をごらんください。

✔ PageScope Data Administrator にて本機にアクセス中その場を離れないでください。やむを得ずその場を離れる場合は、必ず PageScope Data Administrator を終了してください。

1 PageScope Data Administrator の［認証設定 / 宛先設定］モードにて本機にアクセスします。

2 認証設定の展開ボタンをクリックします。

3 ［ユーザー設定］をクリックします。



4 目的の機能を選択します。

➔ ユーザーを登録したい場合は、［追加］をクリックします。

➔ ユーザーの登録内容を変更したい場合は、［編集］をクリックします。

➔ ユーザーを削除したい場合は、［削除］をクリックし、削除実行の確認画面で［はい］をクリックします。

➔ ユーザーパスワードがパスワード規約の条件を満たしていない場合、入力したユーザーパスワードは使用できないことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。パスワード規約について詳しくは、1-8 ページをごらんください。

➔ ユーザー名を入力していない場合、入力していないことを告げるメッセージが表示されます。［OK］をクリックし、ユーザー名を入力してください。

➔ 既に登録済みのユーザー名と同一のユーザー名を重複して登録することはできません。

5 ［OK］をクリックします。

6 ［装置に書込み］をクリックします。

➔ 本機で実行中のジョブまたはジョブ予約（タイマー送信、Fax リダイヤル待ちなど）がされている場合、装置ロックエラーにより書き込みに失敗したことを告げるメッセージが表示されます。［OK］をクリックし、しばらくしてから再度装置への書込みを行ってください。

➔ 手順 4 で登録ユーザーを削除した場合、削除したユーザーの所有する画像ファイルは削除されます。

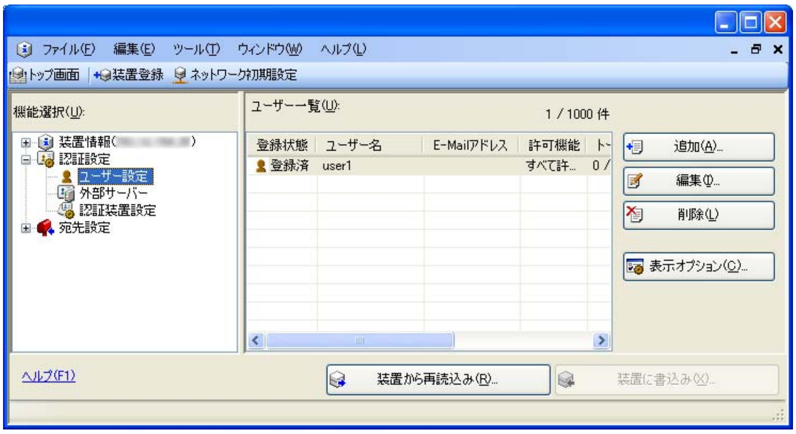
4.1.5 IC カード情報設定のしかた

✔ 事前に管理者の PC に、IC カードリーダーの IC カードドライバー(USB ドライバー)および IC カードプラグインのインストールが必要です。詳しくは本体に同梱のユーザーズガイドをご覧ください。
✔ 本機へのアクセスのしかたは、4-2 ページの手順 1 ～ 5 をごらんください。
✔ PageScope Data Administrator にて本機にアクセス中その場を離れないでください。やむを得ずその場を離れる場合は、必ず PageScope Data Administrator を終了してください。

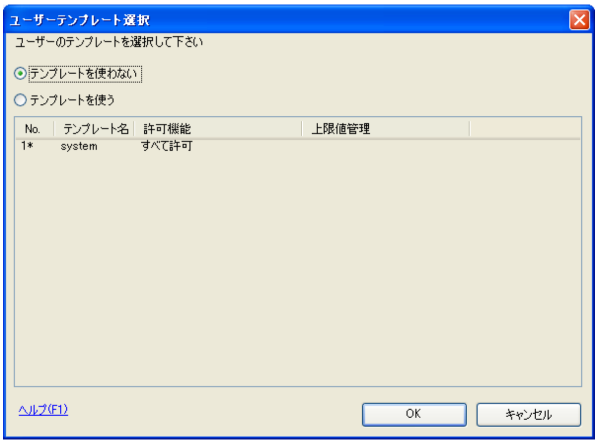
1 PageScope Data Administrator の［認証設定 / 宛先設定］モードにて本機にアクセスします。

2 認証設定の展開ボタンをクリックします。

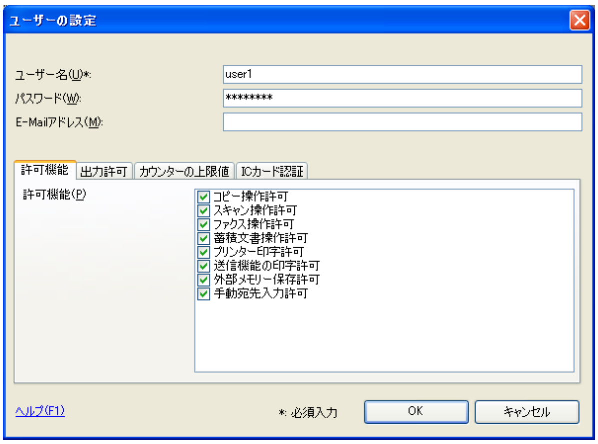
3 ［ユーザー設定］を選択し、［追加］をクリックします。



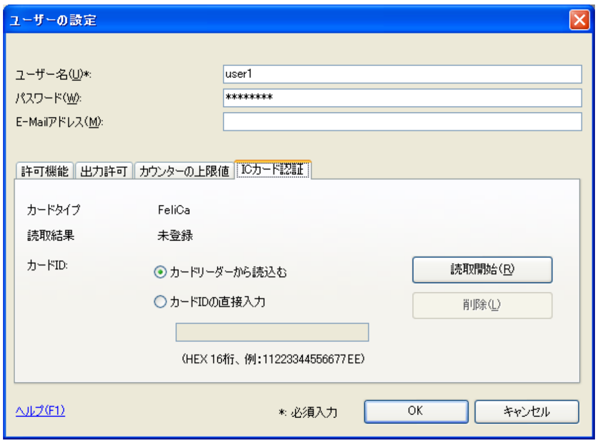
4 ［OK］をクリックします。



5 ユーザー名、パスワードを入力し、［ＩＣ カード認証］タブを選択します。



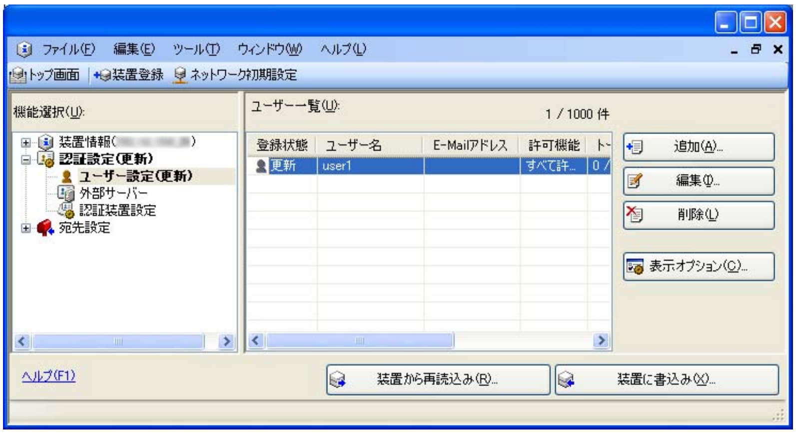
6　ＩＣカードリーダーにＩＣカードを置いて、[読取開始] をクリックします。



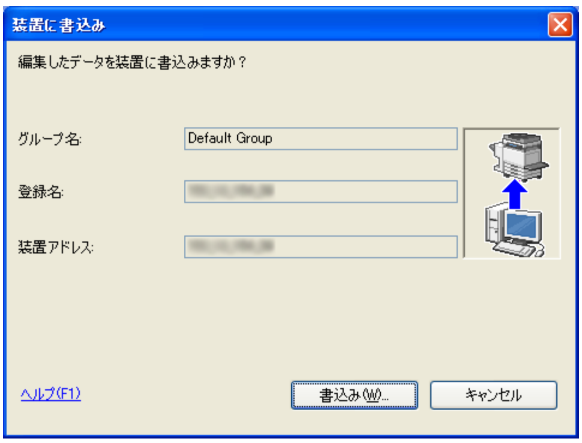
➔ 登録済みの IC カード情報を削除する場合は、[削除] をクリックします。
➔ カード ID を直接入力して登録することもできます。[カード ID の直接入力] のラジオボタンをクリックして、カード ID を入力します。
➔ 直接入力ができる IC カード種類は、「Type A」および「Felica IDm」です。

7　[OK] をクリックします。

8　[装置に書込み] をクリックします。



9　[書込み] をクリックします。



10　[OK] をクリックします。

➔ [カード ID の直接入力] で登録した場合は、本機の管理者設定でユーザーとカードの関連付けが必要です。詳しくは 2-18 ページをごらんください。

4.2　TWAIN ドライバについて

TWAIN ドライバとは、一般ユーザーの PC にインストールし、本機を TWAIN 機器として認識させるための専用 TWAIN ドライバのことをいいます。本機で読み込んだ画像データを PC の画像処理アプリケーションに取り込むことができます。

TWAIN ドライバから本機にアクセスする場合、ユーザーが正当な利用者であることを 8 桁以上 64 桁までのユーザーパスワードを使用して認証します。認証中、入力されたパスワードは、「＊」として表示されます。パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。

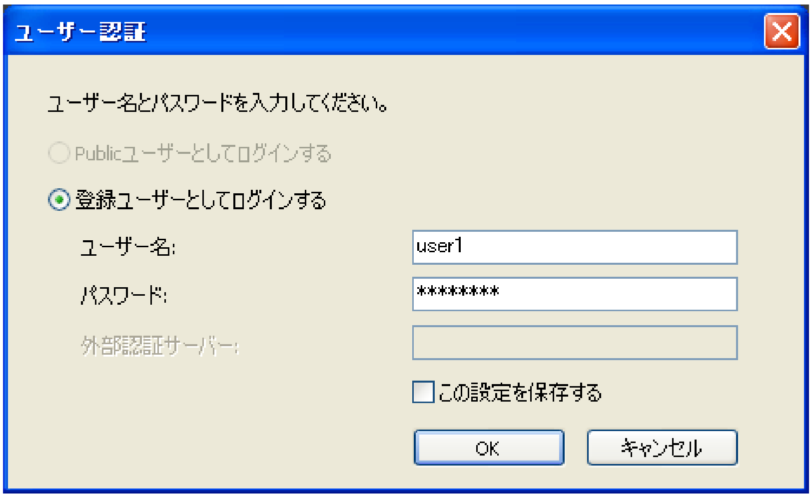
TWAIN ドライバからのアクセスのしかた

✔ TWAIN ドライバにて本機にアクセス中その場を離れないでください。やむを得ずその場を離れる場合は、必ず TWAIN ドライバを終了してください。

1 画像処理アプリケーションを起動させます。

2 ［ファイル］メニューから［読み込み］をクリックし、［KONICA MINOLTA bizhub 42/36 TWAIN（仮称）］を選択します。

3 「登録ユーザーとしてログインする」のラジオボタンをクリックし、ユーザー名および 8 桁以上 64 桁までのユーザーパスワードを入力します。



➔ 認証方式にて［外部サーバー］（Active Directory）が設定されている場合、目的のサーバーを入力してください。

4 ［OK］をクリックします。

➔ ユーザーパスワードを間違えて入力した場合、認証に失敗したことを告げるメッセージが表示されます。正しいユーザーパスワードを入力してください。

➔ パスワード誤入力による認証の失敗は、不正アクセスとしてカウントされます。本機起動中に累積回数が 3 回に達した時点でアクセスロック状態となり、以降のパスワード入力操作を禁止します。アクセスロック状態を解除するには本機電源スイッチの OFF/ON を行ってください。ただし、電源の OFF/ON をする場合は、電源を OFF にして、10 秒以上経過してから ON にしてください。間隔をあけないと、正常に機能しないことがあります。

➔ 認証方式にて［外部サーバー］（Active Directory）が設定されている場合、ユーザー認証にて認証されると、本機に登録されていないユーザー名は自動的に登録されます。

5 各種設定を行い、画像を取り込みます。

お問い合わせは

■ 販売店連絡先

《販売店 連絡先》

販売店名

電話番号

担当部門

担当者

■ 保守・操作・修理・サポートのお問い合わせ

この商品の保守・操作方法・修理・サポートについてのお問い合わせは、お買い上げの販売店、サービス実施店にご連絡ください。

《保守・操作・修理・サポートのお問い合わせ先》

TEL

コニカミノルタ ビジネスソリューションズ株式会社

〒103-0023　東京都中央区日本橋本町1丁目5番4号

当社についての詳しい情報はインターネットでご覧いただけます。　**http://bj.konicaminolta.jp**

当社に関する要望、ご意見、ご相談、その他お困りの点などございましたら、お客様相談室にご連絡ください。
お客様相談室電話番号　フリーダイヤル：0120-805039（受付時間 ： 土、日、祝日を除く9:00〜12:00 / 13:00〜17:00）

KONICA MINOLTA

国内総販売元
コニカミノルタ ビジネスソリューションズ株式会社

製造元
コニカミノルタ ビジネステクノロジーズ株式会社
〒100-0005 東京都千代田区丸の内一丁目6番1号 丸の内センタービルディング

A3EW-9617A-00